APPENDIX A

INTRUSION-DETECTION SYSTEM PERFORMANCE TESTS

Part 1

Exterior Perimeter Sensors

Part 1

Exterior Perimeter Sensors

Objective

The objective of these performance tests is to determine the effectiveness of exterior perimeter sensors. The most directly applicable requirements are:

Applicability	**Order Reference**
Category I and II SNM, Vital Equipment, PA	DOE Manual 5632.1C-1, Chapter VI, Paragraph 4
Classified Matter, LA	OE Manual 5632.1C-1, Chapter VI, Paragraph 4
DOE Property and Unclassified Facilities	DOE Manual 5632.1C-1, Chapter VI, Paragraph 4

System Tested

System - Intrusion-detection system

Function - Perimeter-intrusion detection

Component - Exterior sensors, transmission lines, alarm processing equipment, interfaces with CCTV and CAS operation. Testing and maintenance of perimeter sensors.

Scenario

Inspectors should select one or more zones of a perimeter system for testing based on sensor configuration, terrain, location of buildings and portals, and operating history. A quick tour around the perimeter is helpful in identifying zones and potential deficiencies. Items of interest may include ditches, humps, dips, other terrain variations, obstacles or obstructions, sewer lines, pipes or tunnels that pass under the zone, piping or utility lines that pass over the zone, barriers that could be used as a platform to jump over sensors or to avoid observation, excessive vegetation, and standing water. Particular attention should be paid to the identification of potential gaps in sensor coverage.

The number of sensors and zones selected for testing depends on the time available, the importance of the system in the overall protection program, and the variation in the individual zones. The following guidelines are intended to assist the inspector in the selection of sensors and zones for testing:

- At least two zones should be tested. If the zones employ different sensor configurations, or if the sensor configuration at portals is significantly different, the inspectors should consider selecting at least one of each type.

- At least one of each type of sensor should be tested, if possible. This should include sensors on building roofs and sensors (if any) in tunnels under the perimeter.

- If the first few OA-10 tests do not indicate problems and there is no evidence of exploitable deficiencies, the inspectors should not generally devote extensive time to testing numerous zones and sensors. However, if deficiencies are apparent, the inspectors should collect sufficient data to determine if a deficiency is an isolated instance or evidence of a systemic problem.

- Tests should be conducted for selected zones in which terrain features or questionable installation practices are likely to degrade detection capability.

It is useful for inspectors to observe security alarm technicians or SPOs conducting routine operational or sensitivity tests. Inspectors should determine if the tests, calibrations, and maintenance procedures are consistent with DOE orders and the SSSP, and if they are an effective means of testing the systems. Two goals are accomplished by having the facility's security technicians conduct the routine test prior to testing by the inspectors. First, the facility tests are indicators of the effectiveness of the test and maintenance program. The test procedures can be observed to determine whether they are effective and whether the selected sensors are properly calibrated. Second, the facility tests should verify that the sensors are calibrated according to facility specifications, thus the inspectors will be testing a system that is operating as the facility intends. This may be important in identifying the root cause of any deficiency.

The inspectors may conduct walk tests, crawl tests, run tests, jump tests, climb tests, and step tests, as appropriate, to determine whether an adversary could cross the perimeter without detection and whether the individual sensors are properly calibrated.

Inspectors should monitor the alarm annunciation in the CAS and SAS to determine whether the alarms are functioning properly. The inspectors may also observe the operation of interfacing systems, such as the automatic CCTV display and video recorders.

Evaluation

If the detection system <u>is</u> effective, the sensors <u>will</u> detect intrusion and the alarms <u>will</u> annunciate accordingly.

Assessing Sensor Performance

The primary objective in the evaluation of exterior perimeter intrusion-detection sensors is to determine whether the system effectively and reliably detects an intruder crossing the perimeter. Other questions that should be considered in the evaluation are:

- Do the individual sensors detect an individual crossing the sensor detection pattern at varying rates? Typically the slowest rate for testing should be .15 meter per second and the fastest rate should be 5 meters per second. However, if patrol frequencies and direct visual observation are considered

inadequate to provide reasonable assurance that such attempts would be detected, speed is no longer a factor to consider.

- Are the sensors positioned to allow adversaries to bypass one sensor at a time, or are they positioned such that an adversary attempting to bypass one sensor would be in the detection zone of a second (and possibly a third) type of sensor?

- Does the alarm system annunciate all alarms or does the system incorporate alarm processing logic (for example, one of two, two of three, two of four) that allows one sensor or sensors in different zones to activate without an alarm condition? If so, can adversaries exploit the design, that is, can adversaries cross the perimeter in such a manner that they do not cause an alarm? The inspectors should consider tactics such as zone hopping and defeating one of two complementary sensors.

- Can the adversary exploit the existing barriers (for example, fences, jersey bouncers) as a platform for jumping or as an aid in climbing to avoid detection?

- Have effective measures been taken to protect potential paths under (for example, storm sewers) or over (for example, wires or pipes) the detection zone?

- Are there any seams or bypasses between zones that can be exploited? If so, and there are multiple sensors, can more than one sensor be defeated?

- Are there dips, ditches, humps, or obstructions that could provide a pathway for an individual to avoid detection? If so, can those deficiencies be identified from outside the secure area?

- Are there probable differences in the day and night detection capability due to extremes of heat and cold or effects of sunlight versus darkness?

- Is the detection zone free of snow, ice, standing water, vegetation, or other obstructions that could prevent detection or cause nuisance alarms?

- Are sensors accessible from outside the PA, making them vulnerable to tampering (for example, "nudge" sensors out of alignment; jam multiple infrared or microwave sensors; block CCTV cameras)?

- Are the sensors particularly susceptible to adversaries using tools (for example, ladders, boards, ropes)?

Interpreting Results

The following guidelines are provided to assist the inspectors in interpreting results in the context of system performance.

- A perimeter system is only as good as its weakest link. Tests that indicate that a knowledgeable adversary could frequently cross the perimeter without detection in one or more zones are evidence that the perimeter sensors are not a reliable system. The significance of this finding must be analyzed in the context of the site-specific protection objectives and the effectiveness of other complementary systems.

- In some cases, testing by inspectors indicates that one or more sensors can be defeated but that, because of the degree of redundancy in the sensor configuration, an intruder crossing the perimeter would cause an alarm. In such cases, the identified deficiencies are of lesser concern because the tests

indicate the combination of sensors is effective. However, the sensor deficiencies may indicate testing and maintenance problems.

- In some cases, facility tests indicate that the system is correctly calibrated but inspector tests indicate that the sensors can be defeated or do not reliably detect intrusion. In such cases, it is reasonable to conclude that there are deficiencies in the test and calibration procedures and in the quality assurance program.

- Facility tests that indicate that the sensors are calibrated according to specification, in conjunction with tests by inspectors that confirm the sensors are capable of reliably detecting an intruder, usually signify that the tested portion of the system is effective and that test and maintenance procedures are effective. However, the limitations of the tests must be recognized. For example, not all methods of defeat (for example, bridging of microwave sensors) may have been tested and the test may not have stressed the system to the limit.

- Facility tests that indicate that one or more sensors are not calibrated according to specifications may simply be an indication of an isolated instance of sensor drift. On the other hand, this may indicate systemic problems in the test and maintenance program, or problems related to the age and overall condition of the sensor system. If the facility tests indicate sensors are out of calibration, inspectors should consider instructing the facility technicians to test a representative sample of sensors in order to determine the extent of the problem.

Special Considerations

Some types of sensors are sensitive to the size of the intruder (or more accurately, the radar cross-section). Inspectors should request that the facility provide a relatively small person to conduct the crawl tests.

Related tests or activities, such as perimeter barrier inspections, tests of CCTV and video-recording equipment, and tests of tamper and line supervision alarms, are typically conducted concurrent with the sensor tests.

Responsibilities

Inspectors: Select zones and sensors. Direct tests and monitor alarm annunciation. (Typically one inspector will be stationed at the CAS and at least one at the perimeter.)

Facility: Conduct routine tests. Provide security technicians. Provide test devices as necessary (for example, aluminum spheres). Provide SPOs for security during testing, as required. Provide radios for two-way communication. Provide personnel (normally an SPO) to conduct tests (climb, crawl, run, and walk) at the direction of inspectors.

Internal Coordination

Tests should be scheduled to avoid conflicts with other tests involving the protective force.

Security Considerations

Observe all normal security considerations. Normally, an SPO must monitor (directly or via CCTV) the tests to ensure that no unauthorized personnel enter the protected area.

Personnel Assignments

Test Director:

Facility Alarm System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator (if required):

Facility Safety Coordinator (if required):

Logistical Requirements

Personnel:

- Protective force representative
- Alarm technicians
- Tester

Equipment:

- Radio
- Test devices (for example, aluminum sphere for microwave and calibrated punch for fence vibration sensors)

Safety:

- Follow normal operating procedures
- Complete safety plan (if necessary)
- Notify CAS and other alarm monitoring stations before testing
- Station one inspector in CAS
- Arrange to prevent any undesired armed response to alarms

Bistatic Microwave Sensors

General Characteristics:	Line-of-sight, freestanding, transmitter/receiver pairs
Intruder-Detection Capabilities:	Walking, slow walking, running, crawling, rolling, jumping
Vulnerabilities:	Tunneling, trenching, bridging

Concerns

- Even terrain over the length of the detection zone is critical. Ditches, humps, or dips greater than three inches may significantly reduce the capability to detect a crawling intruder.
- Insufficient offset may allow intruders to crawl under or jump over the beam at the crossover point (the point where adjacent zones overlap; typically, 30 feet or more is required).
- Separation distances between transmitter and receiver that are greater than the effective range of the detector (typically 100 meters) may significantly reduce detection capability.
- Microwave sensors are susceptible to nuisance alarms induced by standing water, high winds, blowing debris, snow, animals, lightning, and fencing that is too close to the sensor beam. Properly drained terrain and well-maintained isolation zones (vegetation free and without holes that would allow large animals to enter) can reduce the nuisance alarm rate.
- The accumulation of snow reduces sensor performance.
- Improper alignment may significantly reduce sensitivity and detection width and contribute to false alarms.
- Transmitters or receivers that are mounted too high may not detect someone crawling under the sensor.
- Transmitters or receivers that are mounted close to the ground may not detect someone vaulting over at the crossover point, if there is insufficient overlap between adjacent zones.

Types of Tests

- Walk Test Across the Zone

  Walk tests or shuffle walk tests are conducted to verify operability and sensitivity, and to determine the width of the detection zone. A shuffle walk involves small slow steps without swinging the arms (steps of five cm or less at .15 m/sec). The width of the detection zone can be determined by monitoring alarm annunciation. Sensitivity tests should be conducted at the mid-range of the sensor beam.

- Walk Test Parallel to the Zone

  Walk tests parallel to the zone are conducted to determine whether the sensor is misaligned or mounted too close to the fence. Such tests involve walking parallel to the zone approximately one meter from the fence and verifying that no alarm occurs.

- Run Tests

  Run tests are conducted to verify whether receiver response is fast enough. Run tests involve crossing the detector zone at a fast run (five m/sec). Such tests are performed where the beam is narrow—approximately six meters from the transmitter or receiver or just inside the crossover point (for overlapping sensors).

- Crawl Tests

  Crawl tests are conducted to verify proper detector alignment and sensitivity, and to determine whether terrain irregularities can be exploited. Crawl tests involve crossing the detection zone at selected points while minimizing radar cross section (intruder remains flat, parallel to the beam, head down, with no reflective clothing). Tests should be conducted by a relatively small individual crawling at approximately .15 m/sec. Tests should be conducted at various points along the detection zone, including just inside the crossover point, at the mid-range, and wherever terrain features are likely to reduce detection.

- Jump Tests

  Jump tests are conducted to verify adequate detection height. Such tests involve attempting to jump over the beam, and are conducted where the beam is narrowest (that is, near the crossover point). Barriers, buildings at the perimeter, sensor posts, or mountings may be used as platforms for jumping.

Test Guidelines

- All tests listed in the previous section should be conducted on at least two typical zones.

- Zones that are substantially different (different terrain, sensor configuration, portals) should also be considered for testing.

- Areas that appear vulnerable (due to alignment, terrain irregularities, or other concerns) should be tested.

- If an individual sensor can be defeated, that same sensor should be retested to determine whether it can be defeated a second time. Several tests of the same sensor may be required to determine whether an adversary can exploit the sensor.

- If an individual microwave sensor can be defeated by one or more methods (for example, jump, run, and crawl), the microwave sensors in other zones should be tested using the same methods in order to determine the extent of the problem. Inspectors should conduct several (three to five) more tests in different zones. If most of these tests indicate that the sensor can be reliably defeated, there is sufficient evidence to indicate that a systemic problem exists. If no other sensors are defeated, one may conclude that an isolated deficiency was identified. If the results are inconclusive, inspectors should consider testing additional sensors. Only rarely would an inspector test more than 10 to 15 zones.

- If the adversary has the knowledge, time, and equipment, bridging or tunneling can defeat all microwave sensors. Such tests should only be conducted if a zone is particularly vulnerable (for example, due to barrier placement, or if patrol frequencies and direct visual observation are considered inadequate to provide reasonable assurance that such attempts are detected).

- Experience with microwave sensors has shown that the slowly crawling intruder and the intruder jumping over a single stack microwave unit are the most difficult to detect. Therefore, much of the testing effort is devoted to crawl tests and jump tests in microwave zones that appear to have alignment problems or terrain irregularities.

Checklist

Bistatic Microwave Sensors

Exterior Perimeter Intrusion-Detection System

Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Sensitivity test frequency _____

_____

Sensitivity test method _____

_____

Acceptance criteria for sensitivity test _____

_____

Procedures for vegetation removal _____

_____

Procedures for snow removal _____

_____

False alarm history/records _____

_____

Make/model _____

_____

Measures to prevent erosion _____

_____

Tamper switches (transmitter, receiver, junction boxes) _____

_____

Tour/Visual Inspection Items

Vegetation present? _____

_____

Deep snow present? _____

_____

Terrain level? _____

_____

Zone length OK? _____

_____

Complements other sensors? _____

_____

Overlap sufficient? _____

_____

Standing water present or likely? _____

_____

Frequency of patrols? _____

_____

Data Collection Sheet
Bistatic Microwave – Exterior Perimeter Intrusion-Detection System

Test Method

	Zone Tested	Zone Number	Walk Across	Walk Shuffle	Walk Parallel	Run	Crawl	Jump
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
Comments:								

Active Infrared Sensors

General Characteristics:	Line-of-sight, vertical plane, post-mounted, multiple transmitters and receivers
Intruder Detection Capabilities:	Walking, slow walking, running, crawling, rolling, jumping
Vulnerabilities:	Tunneling, trenching, bridging, climbing

Concerns

- Because infrared is a narrow beam line-of-sight detector, there should be no surface depressions of six inches or more, which may permit crawling under the lowest transmitter/receiver pair. The bottom beam should be aligned within six inches of the ground surface.

- The ground under the detection zone should be compacted, graveled, or paved to preclude easy furrowing under the zone (look for loose gravel; this is usually a big problem).

- Close proximity to fences, building walls, CCTV towers or other structures may permit easy bridging or jumping over the narrow vertical detection zone (sensor stacks can, themselves, become climbing aids).

- Infrared sensors are susceptible to nuisance alarms induced by animals, vegetation, fog, snow, and wind-blown dust and debris.

- Heavy snow must be removed to preclude tunneling through the snow to avoid detection.

- In some older model sensors, sunlight and vehicle headlights may cause false alarms.

- Improper alignment may significantly reduce sensitivity and detection width and contribute to false alarms.

Types of Tests

- Walk Test Across the Zone

  Walk tests are conducted to verify operability and sensitivity. These tests should be conducted at mid-range of the sensor beam.

- Run Tests

  Run tests are conducted to verify that receiver response is fast enough. They involve crossing the detector zone at a fast run (5 m/sec).

- Crawl Tests

  Crawl tests are conducted to verify proper detector alignment and sensitivity, and to determine whether terrain irregularities can be exploited. Crawl tests involve crossing the detection zone at selected points while

minimizing target cross-section (intruder remains flat, perpendicular to the beam, head down, with no reflective clothing). Tests should be conducted by a relatively small individual moving at approximately .15 m/sec (see "Assessing Sensor Performance," page A-2). Tests should be conducted at various points along the detection zone, including the mid-point, and wherever terrain features are likely to reduce detection capability.

- Jump Tests

  Jump tests are conducted to verify adequate detection height. Such tests involve attempting to jump over the beam and are conducted where barriers, buildings, sensor posts, or mountings can be used as jumping platforms.

Test Guidelines

- All the tests listed in the previous section should be conducted on at least two typical zones.
- Zones that are substantially different (different terrain, sensor configuration, or portals) should also be considered for testing.
- Areas that appear vulnerable (due to structures that aid bridging or jumping, terrain features, or other concerns) should be tested.
- If an individual sensor can be defeated, that same sensor should be tested again to determine whether such defeat can be repeated. Several tests of the same sensor may be required to determine whether an adversary can reliably exploit a sensor deficiency.
- If an individual zone can be defeated by one or more methods (for example, jump, run, crawl) other zones should be tested using the same methods to determine the extent of the problem. The inspectors should conduct several (three to five) more tests in different zones. If most of these tests indicate the sensor can be reliably defeated, it is likely that a systemic problem exists. If no other sensors are defeated, one may conclude that an isolated deficiency was identified. If results are inconclusive, the inspectors should consider testing additional sensors. Only rarely would an inspector test more than 10 to 15 zones using the same methods.
- If the adversary has the knowledge, time, and equipment, bridging or tunneling techniques can defeat all infrared sensors. Since the infrared beam is quite narrow, bridging or tunneling can be accomplished fairly rapidly and easily. Such tests should only be conducted if a zone is particularly vulnerable (for example, due to barrier placement) or if patrol frequencies and direct visual observation (CCTV or guard posts) are considered inadequate to provide reasonable assurance that such attempts are detected.
- Experience with infrared sensors has shown that vaulting the zone at the mounting post is the most likely method of quickly defeating the system. This method, together with the crawl test (where there are depressions in the ground surface), should be used when possible.

Checklist

Active Infrared Sensors

Exterior Perimeter Intrusion-Detection System

Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Sensitivity test frequency _____

_____

Sensitivity test method _____

_____

Acceptance criteria for sensitivity test _____

_____

Procedures for vegetation removal _____

_____

Procedures for snow removal _____

_____

False nuisance alarm history/records _____

_____

Make/model _____

_____

Measures to prevent erosion _____

_____

Tamper switches (transmitter, receiver, junction boxes) _____

_____

Tour/Visual Inspection Items

Vegetation present? _____

_____

Deep snow present? _____

_____

Terrain level? _____

_____

Zone length OK? _____

_____

Complements other sensors? _____

_____

Overlap sufficient? _____

_____

Structures adjacent to the zone permitting vaulting/bridging _____

_____

Data Collection Sheet
Active Infrared Sensors – Exterior Perimeter Intrusion-Detection System

Test Method

	Zone Tested	Zone Number	Walk	Run	Crawl	Jump	Bridge
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
Comments:							

Electric Field Sensors

General Characteristics:	Electric field-generating wire coupled to sensor wire, freestanding or fence-mounted, can follow irregular terrain
Intruder Detection Capabilities:	Walking, slow walk, running, crawling, rolling, jumping
Vulnerabilities:	Tunneling, trenching, bridging

Concerns

- Improper wire/spring tension or improper wire/insulation coupling can cause unacceptable false and nuisance alarms. Careful installation and maintenance are required for proper sensor operation.

- Two-wire (versus three- or four-wire) configurations may permit an intruder to jump between the field wire and sensing wire undetected.

- When more than one section of electric field is installed, adjacent sensors should overlap to overcome the lack of sensitivity around the tension springs and end insulators.

- Electric field sensors are not generally used at fence gates because of the requirement to maintain wire tension, although removable sections can be used. For frequently used gates, active infrared or microwave sensors are normally used. In such cases, there must be sufficient overlap between the gate sensor and the adjacent electric field zone to preclude intrusion between zones of different sensors.

- Electric field sensors are susceptible to nuisance alarms from lightning, high-level electromagnetic noise (for example, transformers) animals, heavy rain, wet snow, and blowing debris.

Types of Tests

- Walk Test Perpendicular to the Zone

  Walk tests are used to verify sensor operability and sensitivity. The zone should alarm when approached at normal walking speed when one is between 1 and .5m from the wire. This test is used for two- and three-wire systems (see "Assessing Sensor Performance," page A-2).

- Shuffle Walk Test Perpendicular to the Zone

  Shuffle tests are conducted by taking slow, small steps without swinging the arms (steps of 5 cm or less at .15 m/sec). The system should alarm at a distance of 25 cm or less, and any attempt to climb between the wires should be detected.

- Stoop Test (for four-wire systems)

  This test is conducted by walking to a point near the sensor then facing parallel to the wires. The control unit should be allowed to stabilize, then the individual should stoop or squat down to unbalance the upper and lower zones. An alarm should annunciate.

- Crawl Test Perpendicular to the Zone

  The crawl test consists of an individual crossing the zone at a slow crawl as close to the ground as possible, in zones where the bottom wire is highest (6 inches or more) from the ground or where there is a depression in the zone. An alarm should annunciate.

- Jump Test

  The jump test cannot normally be performed if the electric field sensor is properly installed, due to the height of the detection zone (eight feet or more). However, where there are structures adjacent to the zone it may be possible to jump over the sensor wire, if personal safety can be assured.

- Step-Through Test

  Step-through tests should be conducted if the walk tests, shuffle walk tests, and stoop tests indicate that the electric field sensors are not sufficiently sensitive. The step-through test consists of an individual stepping or jumping between the electric field wires and crossing the detection zone while avoiding contact with the wire. If the zones do not overlap, this test should be conducted at the end of the zone (near tension springs) where sensitivity is lowest, otherwise the test should be conducted at several locations throughout the zone. Some of the older models are more susceptible to penetration.

Test Guidelines

- The person conducting the tests should remove all metal objects and should not wear steel-toed shoes or wear gloves.

- Walk tests, shuffle walk tests, and stoop tests should be conducted on at least two typical zones.

- If sensitivity is questionable on the initial walk or stoop tests, the step-through tests should be conducted to determine if a person can cross the detection zone undetected.

- Zones that are substantially different (different terrain, sensor configuration, portals) should also be considered for testing.

- Areas that appear vulnerable (due to terrain features or other concerns) should be tested (crawl tests or jump tests).

- If an individual sensor can be bypassed, that same sensor should be tested again to determine if bypassing can be repeated. Several tests of the same sensor may be required to determine if an adversary can reliably exploit the sensor deficiency.

- If an individual electric field zone can be defeated by one or more methods (for example, jumping, running, crawling), other zones should be tested using the same methods to determine the extent of the problem. The inspectors should conduct several more tests (three to five) in different zones. If most of these tests indicate that the sensor can be reliably defeated, it is likely that there is a systemic problem. If no other sensors are defeated, it may be concluded that an isolated deficiency was identified. If the results are inconclusive, additional sensors may be considered for testing. Only rarely would an inspector test more than 10 to 15 zones using the same method.

- If an adversary has the knowledge, time, and equipment, bridging or tunneling can defeat all electric field sensors. Such tests should only be conducted if it appears that a zone is vulnerable, or if patrol frequencies and direct visual observation (CCTV or guard posts) are considered inadequate to provide reasonable assurance that such attempts are detected.

- Experience with electric field sensors has shown that the slow-crawling intruder is the most difficult to detect. Typically, much of the test effort is devoted to crawl tests of zones that appear to have installation or terrain irregularities.

Checklist

Electric Field Sensors

Exterior Perimeter Intrusion-Detection System

Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Sensitivity test frequency _____

_____

Sensitivity test method _____

_____

Acceptance criteria for sensitivity test _____

_____

Procedures for vegetation removal _____

_____

Procedures for snow removal _____

_____

False alarm history/records _____

_____

Make/model _____

_____

Measures to prevent erosion _____

_____

Tamper switches (transmitter, receiver, junction boxes) _____

_____

Tour/Visual Inspection Items

Vegetation present? _____

_____

Deep snow present? _____

_____

Terrain level? _____

_____

Zone length OK? _____

_____

Complements other sensors? _____

_____

Overlap sufficient? _____

_____

Wire tension and terminations satisfactory? _____

_____

Data Collection Sheet
Electric Field Sensors – Exterior Perimeter Intrusion-Detection System

Test Method

	Zone Tested	Zone Number	Walk	Walk Shuffle	Stoop	Crawl	Jump	Step Through
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
Comments:								

Buried Line Sensors

General Characteristics:	Buried cable(s); seismic, magnetic or electromagnetic coupled field detectors; signal processor unit; cable(s) follow terrain
Intruder-Detection Capabilities:	Varies depending on type; may include walking, running, jumping, crawling, trenching, and tunneling
Vulnerabilities:	Bridging

Note: Due to the varying sensing techniques of buried line sensors, the strengths and weaknesses of various systems differ somewhat. However, the method of testing is the same for each.

Concerns

- Standing water, wind-blown debris, electromagnetic interference, vehicular traffic, lightning, and animals may cause nuisance alarms depending on the type of buried line sensor used.
- Seismic sensors may not function when installed under roadbeds or sidewalks, or when the ground is frozen or under deep snowpack.
- Ported leaky coax is susceptible to nuisance alarms due to running or wind-blown water, moving metallic objects (vehicles), or lightning.
- Seismic sensors may experience nuisance alarms if installed in the vicinity of fences, power poles, guy-wires, or roads (vehicle ground vibration).
- Ground covering the sensor should be maintained in such a manner that the actual location of the sensor is not visually apparent.

Types of Tests

- Walk Tests Across the Zone

  Walk tests should be conducted at a normal walking speed in at least three places within each buried cable zone.

- Run or Jump Tests Across the Zone

  Run tests are conducted to verify prompt sensor response and should be conducted at a fast run (5m/sec) at three locations within a given detection zone. The runner may attempt to jump over the location where the sensor is buried.

- Roll Tests to the Zone

  Roll tests consist of an individual slowly rolling across the detection zone with the body oriented parallel to the buried cable(s) with arms held close to the body and legs together. A roll test should be conducted when there is a hard surface road or sidewalk crossing the zone.

Test Guidelines

- All tests listed in previous section should be conducted on at least two typical zones.

- Areas that appear vulnerable (due to the existence of hard surface roads, standing water, sources of seismic interference, or other reasons) should be tested.

- If an individual sensor can be defeated, that same sensor should be tested again to determine whether it can be defeated again. Several tests of the same sensor may be required to determine if an adversary can reliably exploit the sensor.

- If an individual zone can be defeated by one or more methods, the buried line sensors in other zones should be tested using the same methods to determine the extent of the problem. Inspectors should conduct several more tests (three to five) in different zones. If most of these tests indicate that the sensor can be reliably defeated, it is likely that a systemic problem exists. If no other sensors are defeated, one may conclude that an isolated deficiency was identified. If the results are inconclusive, additional testing should be considered. An inspector would rarely test more than 10 to 15 zones using the same methods.

- If the adversary has the knowledge, time, and equipment, bridging techniques can defeat most buried line sensors. Such tests should only be conducted if a zone is particularly vulnerable, or if patrol frequencies and direct visual observation (CCTV or guard posts) are considered inadequate to provide reasonable assurance that such attempts are detected.

Checklist

Buried Line Sensors

Exterior Perimeter Intrusion-Detection System

Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Sensitivity test frequency _____

_____

Sensitivity test method _____

_____

Acceptance criteria for sensitivity test _____

_____

Procedures for vegetation removal _____

_____

Procedures for snow removal _____

_____

False alarm history/records _____

_____

Make/model _____

_____

Tamper switches (transmitter, receiver, junction boxes) _____

_____

Tour/Visual Inspection Items

Vegetation present? _____

_____

Deep snow present? _____

_____

Terrain level? _____

_____

Zone length OK? _____

_____

Complements other sensors? _____

_____

Overlap sufficient? _____

_____

Standing water present or likely? _____

_____

Hard surfaced road crosses zone? _____

_____

Power poles, guy wires or other seismic sources exist? _____

_____

Data Collection Sheet
Buried Line – Exterior Perimeter Intrusion-Detection System

Test Method

	Zone Tested	Zone Number	Walk	Run/Jump	Roll
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
Comments:					

Taut-Wire Sensor Fence

General Characteristics:	Tensioned horizontal wires connected to detector posts, freestanding or fence-mounted
Intruder Detection Capabilities:	Cutting, climbing, or other deflection of sensor wire
Vulnerabilities:	Tunneling, trenching, bridging

Concerns

- Since taut-wire sensors operate on mechanical principles, they are relatively impervious to weather, wind, electromagnetic interference, and other common sources of nuisance alarms.

- Some systems, which have only one sensor switch channel for multiple parallel switches, may be defeated by cutting ungrounded switch leads if the end-of-line resistor and signal cable are not disturbed.

- As with other fence-mounted mechanical (pressure, strain, vibration) sensors, taut-wire systems are susceptible to defeat by tunneling, bridging, or jumping, if no physical contact with the sensing wires occurs.

- Taut-wire sensors are not generally used at fence gates because of the requirement to maintain wire tension. For frequently used gates, active infrared or microwave sensors are often used. In such cases, there must be sufficient overlap between the gate sensor and the adjacent taut-wire zone to preclude intrusion between zones of different sensors.

- Older systems used fewer total wires, allowing inspectors to climb over system or under system if not fence-mounted.

Types of Tests

- Simulated Climb Test (for freestanding taut-wire sensors)

  This test consists of a ladder being placed against the wires and an individual climbing the ladder to a point where sensor activation occurs (usually when the knees are near the top of the fence). Local alarm indication is required to prevent damage to sensor switches.

- Wire Pull Test

  Individual wires are pulled up or down by hand so that a deflection of approximately four inches is achieved. The distance that the wire is pulled before an alarm is generated should be noted.

- Cutting

  No actual cutting of the sensor wires should be performed.

- Jump Tests

  These tests cannot normally be performed if the taut-wire sensor is properly installed, due to the height of the detection zone (eight feet or more). However, structures adjacent to the zone used as platforms may make it possible to jump over the sensor wire, if personal safety can be assured.

Note: During periods of extreme cold weather, it may take some time for the mechanical sensor switches to return to the normal neutral position after activation. This should be taken into account when considering multiple tests of the same zone.

Test Guidelines

- All tests listed in the previous section should be conducted on at least two typical zones.

- Zones that are substantially different (different terrain, sensor configuration, portals) should also be considered for testing.

- Areas that appear vulnerable (due to terrain irregularities or other reasons) should be tested to determine whether a vulnerability exists.

- If an individual sensor can be defeated, that same sensor should be tested again to determine if it can be defeated repeatedly. Several tests of the same sensor may be required to determine whether an adversary can reliably exploit the sensor deficiency.

- If an individual taut-wire zone can be defeated by one or more methods (for example, bridging and climbing), other zones should be tested using the same methods to determine the extent of the problem. Inspectors should conduct several more tests (three to five) in different zones. If most of these tests indicate that the sensor can be reliably defeated, it is likely that a systemic problem exists. If no other sensors are defeated, one may conclude that an isolated deficiency was identified. If results are inconclusive, additional testing should be considered. Only rarely would an inspector test more than 10 to 15 zones using the same methods.

- If the adversary has the knowledge, time, and equipment, bridging or tunneling techniques can defeat all taut-wire sensors. Such tests should be conducted only if a zone is particularly vulnerable (for example, due to barrier placement), or if patrol frequencies and direct visual observation (CCTV or guard posts) are considered inadequate to provide reasonable assurance that such attempts are detected.

Checklist

Taut-Wire Sensor Fence

Exterior Perimeter Intrusion-Detection System

Interview Items

Installation location _____

_____

Frequency of operational test _____

_____

Operational test method _____

_____

Sensitivity test frequency _____

_____

Sensitivity test method _____

_____

Acceptance criteria for sensitivity test _____

_____

Procedures for vegetation removal _____

_____

Procedures for snow removal _____

_____

False alarm history/records _____

_____

Make/model _____

_____

Measures to prevent erosion _____

_____

Tamper switches (junction boxes) _____

_____

Tour/Visual Inspection Items

Vegetation present? _____

_____

Deep snow present? _____

_____

Terrain level? _____

_____

Zone length OK? _____

_____

Complements other sensors? _____

_____

Overlap sufficient? _____

_____

Wire tension and terminations satisfactory? _____

_____

Data Collection Sheet
Taut-Wire Sensor Fence – Exterior Perimeter Intrusion-Detection System

Test Method

	Zone Tested	Zone Number	Simulated Climb	Wire Pull	Cutting	Jump
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
Comments:						

Video Motion Detector

General Characteristics:	Comparison of digitized camera view, some masking capability, variable scan rates
Intruder Detection Capabilities:	Any intruder motion affecting a sufficient part of the camera's field of view
Vulnerabilities:	Extreme slow motion and an individual wearing clothing that matches the background

Concerns

- Video motion detectors are complex devices requiring extensive maintenance and calibration.
- Due to high detection sensitivity, some systems are highly susceptible to nuisance alarms from reflected light, cloud motion, sunrise and sunset, automobile headlights, wind-blown objects, and animals (if the detector's field of view is wide and encompasses areas outside of the potential space, the greater the potential for nuisance alarms).
- Camera vibration due to wind may create false alarms, as well as improper camera signal synchronization or other video signal disturbance.
- Camera image tube "burn in" caused by a constant view of the same scene may degrade sensitivity of the video motion detector, particularly where extreme changes in light to dark contrast are present.
- Any obstruction that blocks the camera's field of view, or creates strong shadowed areas, may prevent intruder detection.
- If the length of the field of view is too long for the camera lens, an intruder at the extreme end of the field of view may be able to avoid detection.
- If the "refresh rate" (the rate at which one camera scene is compared to the previous scene) is too slow, an intruder may be able to run through the field of view near a camera without detection.
- In the case of digital systems, the zone(s) of detection should be reviewed to ensure proper coverage in the field of view.
- Fog or smoke (grenade) is likely to adversely impact system effectiveness.

Types of Tests

- Walk Test Across the Zone

  Walk tests or shuffle-walk tests are conducted to verify operability and sensitivity, and to determine the width of the detection zone. A shuffle walk involves small slow steps without swinging the arms (steps of 5 cm or less at .15 m/sec.). Width of the detection zone can be determined by monitoring alarm annunciation. Sensitivity tests should be conducted at the furthermost observable point in the camera's field of view (see "Assessing Sensor Performance," page A-2).

- Run Tests

  Run tests are conducted to determine whether the detector response is fast enough. Run tests consist of an individual crossing the detector zone at a fast run (5 m/sec). Such tests are performed at the nearest and furthermost points in the camera's field of view (see "Assessing Sensor Performance," page A-2).

- Crawl Tests

  Crawl tests are conducted to verify proper detector sensitivity and to determine whether terrain irregularities can be exploited. Crawl tests consist of an individual crossing the detection zone at selected points (intruder remains flat, parallel to the camera field of view, head down, with no reflective clothing). Tests should be conducted by a relatively small individual moving at approximately .15 m/sec. Tests should be conducted at various points along the detection zone wherever terrain features are likely to reduce detection and at the furthermost observable point in the camera's field of view (see

Note: Cameras outside the protected area can be manipulated to prevent alarming during intrusion. Special care must be taken when examining a video motion detector system with unprotected cameras.

Test Guidelines

- Tester should be dressed in standard work clothing (e.g., washed denim jeans and jacket).
- Camouflage will assist the tester (snow camouflage in snow or light-colored gravel).
- All tests listed in the previous section should be conducted on at least two typical zones.
- Zones that are substantially different (different terrain, lighting conditions, obstructions) should also be considered for testing.
- Areas that appear vulnerable (due to lighting deficiencies, terrain irregularities, or other reasons) should be tested to determine whether a vulnerability exists.
- If an individual camera's detector can be defeated, that same camera should be tested again to determine whether the deficiency can be repeated. Several tests of the same zone may be required to determine whether an adversary can reliably exploit the deficiency.
- If an individual camera zone can be defeated by one or more methods (run, walk, crawl), the other camera zones should be tested using the same methods to determine the extent of the problem. The inspectors should conduct several more tests (three to five) in different zones. If most of these tests indicate the detector can be reliably defeated, it is likely that there is a systemic problem. If no other zones are defeated, one may conclude that an isolated deficiency was identified. If the results are inconclusive, additional testing should be considered. Rarely would an inspector test more than 10 to 15 zones using the same methods.

Checklist

Video Motion Detector

Exterior Perimeter Intrusion-Detection System

Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Sensitivity test frequency _____

_____

Sensitivity test method _____

_____

Acceptance criteria for sensitivity test _____

_____

Procedures for vegetation removal _____

_____

Procedures for snow removal _____

_____

False nuisance alarm history/records _____

_____

Make/model _____

_____

Measures to prevent erosion _____

_____

Tamper switches (transmitter, receiver, junction boxes) _____

_____

Tour/Visual Inspection Items

Vegetation present? _____

_____

Deep snow present? _____

_____

Terrain level? _____

_____

Zone length and field of view OK? _____

_____

Complements other sensors? _____

_____

Overlap sufficient? _____

_____

Obstructions present? _____

_____

Lighting adequate? _____

_____

Data Collection Sheet
Video Motion Detection – Exterior Perimeter Intrusion-Detection System

Test Method

	Zone Tested	Functional Test	Walk	Run	Crawl
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
Comments:					

Monostatic Microwave Sensors

General Characteristics:	Volumetric coverage; transmitter/receiver unit; typically mounted pointing at a building to provide coverage of approaches; also used on rooftops or gates
Intruder Detection Capabilities:	Walking, slow walk, running, crawling, rolling, jumping
Vulnerabilities:	Tunneling, trenching, bridging

Concerns

- Microwave sensors are susceptible to false alarms induced by standing water, high winds, snow, animals, lightning, and fencing that is too close to the sensor beam. Properly drained terrain and well-maintained isolation zones (vegetation free and without holes that would allow large animals to enter) can reduce the false alarm rate.

- Optimum coverage requires direct line of sight. Obstructions such as columns, beams, air-conditioning units, or other large objects may prevent detection.

- Sensor transceivers and control units are subject to physical damage and tampering if they are readily accessible or are not covered by another sensor's detection pattern.

- Sensors are susceptible to false alarms due to moving objects, electromagnetic radiation, air movement, seismic vibration, fluorescent lighting, and background noise.

- Proper overlap and coverage must be considered to ensure that an intruder cannot cross over, around, or under the sensor's pattern of coverage.

- The microwave detection beam can easily penetrate glass, wood, wallboard, and plastic (including downspouts and drainpipes), creating false alarms from moving objects outside the protected space.

- A sensor is most sensitive to a target moving directly toward or away from the transceiver.

- Inspector should check to see if sensor could be deliberately misaligned. It will reset itself regardless of position (i.e., point at the sky)—insider or outsider.

Types of Tests

- Sensitivity Walk Test

  Walk tests are used to verify operation and sensitivity of the sensor. This test is performed by slowly walking (1 ft/sec) toward microwave sensors until an alarm is received. This test should establish the far end of the sensor coverage pattern.

Crossing Walk Test

This test verifies the ability of the sensor to detect motion along the least sensitive axis of the detection pattern. After the end of the sensor coverage pattern is determined from a sensitivity walk test, a crossing test should be performed by walking across the far end of a microwave zone from various points outside the detection zone. Detection should occur before the tester enters the defined protected space or reaches the protected asset.

- Avoidance Walk Test

  Based on the sensor coverage pattern (oval, wedge, or circle), the inspector should attempt to enter the target zone by walking around the sensor's zone of coverage. This test should verify adequate sensor coverage and overlap to provide detection for the protected space or target/object.

- Crawl test—as close to sensor head as possible.

Test Guidelines

- The person conducting the tests should remove all metal objects and should not wear steel-toed shoes. Observers should be requested to stand away from the area being tested in order to reduce confusion.

- Testing should be conducted on at least two typical zones.

- Any zones that have potential vulnerabilities caused by obstructions or other sources of interference should be tested to determine whether they can be exploited.

- If there are apparent weaknesses in zone coverage or sensor overlap, these should be tested to determine whether sensor coverage could be circumvented.

- Experience indicates that monostatic microwave sensors are most vulnerable to a very slowly moving target entering the detection zone on the least sensitive axis (across the zone for microwave sensors).

- Many sensors have alarm indicator lights built into the sensor head. The inspectors may observe these indicators to facilitate testing the coverage pattern or sensor sensitivity. However, the inspectors should also verify that an alarm is received in the alarm stations to ensure that the alarm circuit is functional from sensor to annunciation point.

- If an individual sensor can be defeated, that same sensor should be tested again to determine whether the deficiency can be repeated. Several tests of the same sensor may be required to determine if an adversary can reliably exploit the sensor deficiency.

- If an individual microwave sensor or zone can be defeated, the microwave sensors in other zones should be tested using the same methods to determine the extent of the problem. The inspectors should conduct several more tests (three to five) in different zones. If most of these tests indicate that the sensor can be reliably defeated, it is likely that a systemic problem exists. If no other sensors are defeated, one may conclude that an isolated deficiency was identified. If results are inconclusive, additional testing should be considered.

Checklist

Monostatic Microwave Sensors

Exterior Perimeter Intrusion-Detection System

Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Sensitivity test frequency _____

_____

Sensitivity test method _____

_____

Acceptance criteria for sensitivity test _____

_____

Procedures for vegetation removal _____

_____

False alarm history/records _____

_____

Make/model _____

_____

Tamper switches (transmitter, receiver, junction boxes) _____

_____

Tour/Visual Inspection Items

Vegetation present? _____

_____

Complements other sensors? _____

_____

Overlap sufficient? _____

_____

Standing water present or likely? _____

_____

Obstructions present? _____

_____

Data Collection Sheet
Monostatic Microwave Sensors – Exterior Perimeter Intrusion-Detection System

Test Method

	Zone Tested	Sensitivity Walk	Crossing Walk	Avoidance Walk	Crawl
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
Comments:					

Fence Disturbance Sensors

General Characteristics:	Sensing wires/cables attached to or woven through fence, sonic capacitance, or piezoelectric technologies
Intruder Detection Capabilities:	Cutting, climbing, or other vibration/deflection of sensor wire or fence
Vulnerabilities:	Tunneling, trenching, bridging

Concerns

- Fence disturbance sensors are susceptible to defeat by tunneling, bridging, or jumping, if no physical contact with the sensing wires occurs.

- Depending on the sensitivity setting, fence disturbance sensors may be susceptible to high false alarm rates. Common causes of false alarms include high winds, animals, and other sources of fence vibration. It is important that fences, gates, outriggers, and barbed wire be mechanically sound and well-maintained to prevent excessive fence vibration.

- In some sensor designs, the sensing wires are least sensitive near the terminal connections and corners.

- The sensor wire or sensors must contact the fence for reliable, nuisance alarm-free performance. It is important that the sensors and/or cabling be attached per manufacturer specifications.

Types of Tests

- Unaided Climb Test

  The test consists of an individual (preferably a small individual) climbing the fence at various locations to verify that detection occurs. Attempts should be made near fence posts, especially corners/posts.

- Ladder Climb Test

  A ladder is placed against the fence. An individual climbs the ladder to the point of sensor activation.

- Cutting Attack

  No actual cutting of the sensor wires or fence fabric should be performed.

- Jump Tests

  These tests cannot normally be conducted if a fence disturbance sensor is properly installed, due to the height of the detection zone (eight feet or more). However, adjacent structures used as platforms may permit an individual to jump over the fence/sensor wire, if personal safety can be ensured.

Test Guidelines

- All the unaided climb tests should be conducted on several fence posts in at least two typical zones.

- Zones that are substantially different (gates or different sensor configuration) should also be considered for testing.

- Areas that appear vulnerable to jumping should be tested to determine whether a vulnerability exists. Safety concerns should be addressed.

- If an individual sensor can be defeated, that same sensor should be tested again to determine whether the deficiency can be repeated. Several tests of the same sensor may be required to determine whether an adversary can reliably exploit the sensor deficiency.

- If an individual zone can be defeated, other zones should be tested using the same methods to determine the extent of the problem. The inspectors should conduct several (three to five) more tests in different zones. If most of these tests indicate that the sensors can be reliably defeated, it is likely that there is a systemic problem. If no other sensors are defeated, one may conclude that an isolated deficiency was identified. If the results are inconclusive, additional testing should be considered. Rarely would an inspector test more than 10 to 15 zones using the same methods.

- If the adversary has sufficient knowledge, time, and equipment, bridging or tunneling techniques can defeat all fence disturbance sensors. Such tests should only be conducted if a zone is particularly vulnerable (for example, due to barrier placement), or if patrol frequencies and direct visual observation (CCTV or from guard posts) are considered inadequate to provide reasonable assurance that such attempts are detected.

Checklist

Fence Disturbance Sensors

Exterior Perimeter Intrusion-Detection System

Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Sensitivity test frequency _____

_____

Sensitivity test method _____

_____

Acceptance criteria for sensitivity test _____

_____

False alarm history/records _____

_____

Make/model _____

_____

Measures to prevent erosion _____

_____

Tamper switches (transmitter, receiver, junction boxes) _____

_____

Tour/Visual Inspection Items

Vegetation present? _____

_____

Zone length OK? _____

_____

Complements other sensors? _____

_____

Overlap sufficient? _____

_____

Data Collection Sheet
Fence Disturbance Sensors – Exterior Perimeter Intrusion-Detection System

Test Method

	Zone Tested	Unaided Climb	Ladder Climb	Cutting	Jump
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
Comments:					

This page is intentionally left blank.

Part 2

Interior Sensors

Part 2

Interior Sensors

Objective

The objective is to test the effectiveness of interior sensors in detecting adversary intrusion. The most directly applicable DOE requirements are given below.

Applicability	Order Reference
Category I and II SNM, Vital Equipment, Vital Areas, MAAs	DOE Manual 5632.1C-1 Chapter VI, Paragraph 3
Classified Matter	DOE Manual 5632.1C-1 Chapter VI, Paragraph 3
DOE Property and Unclassified Facilities	DOE Manual 5632.1C-1 Chapter VI, Paragraph 3

System Tested

System - Intrusion-detection system

Functional Element - Interior intrusion detection

Component(s) - Interior sensors, transmission lines, alarm processing equipment, interfaces with CCTV and CAS operation. Testing and maintenance of interior sensors.

Scenario

The inspectors should select several interior locations (MAAs, vaults, vital areas, or vault-type rooms) for testing, based on a number of factors: sensor types used, construction type, materials, configuration of the interior area, and operating history of the various sensors. At least one of each type of room or vault configuration and sensor should be tested.

The inspectors should review building layouts and architectural drawings. They should also briefly tour the facility to familiarize themselves with typical protection system configurations and to identify potential weaknesses. The relationship between sensor application and the types of structural barriers in use should be noted. The detection capabilities of individual sensor types may vary depending upon the types of barriers used and the ability of these barriers to resist or delay penetration. Also, since some sensors respond to physical attacks on the barrier material, it is important that the detection technology employed (for example, acoustic, vibration, strain, or capacitance technologies) be suited to the barrier material used.

In general, sensors will be of three generic types: motion (or area), barrier penetration, and proximity. Each of these types is subject to various physical and environmental limitations that must be considered when assessing suitability and operating performance. Limitations involve electromagnetic, radiological, acoustical, seismic, thermal, and optical effects, as well as the physical limitations imposed by equipment placement, room arrangement, and building materials used in walls, ceilings, floors, windows, doors, and penetrations (for example, ductwork and cable chases).

The inspectors should observe, if possible, alarm technicians or SPOs during the conduct of routine operational and sensitivity tests of selected sensors. The inspectors should base their selection of the sensors to be tested on the number, type, configuration, and operational history of those sensors. During this portion of the test, inspectors should observe calibration and maintenance procedures to determine whether they are consistent with DOE orders and approved SSSPs. In addition, observation of these tests may indicate the effectiveness of the test and maintenance program. Observations of facility-conducted tests are helpful in identifying the root causes of many noted deficiencies.

The inspectors should conduct standard walk tests and tamper-indicating tests (provided no physical damage to the sensor will result) for each motion detection (area type) sensor tested. Barrier sensors (magnetic switches, glass sensors, and capacitance devices) and proximity sensors may require other tests as applicable and as identified in manufacturer's instructions. The purpose of these tests is to determine whether each sensor type is functioning, whether it can detect attempted tampering, and whether it can detect its design basis target (intruder) or activity (for example, attempted barrier penetration using force or attack tools).

Within a single area, there may be several types of sensors having different detection goals. For example, some barriers may have a penetration detection sensor, a volumetric area sensor for the interior, and a proximity or capacitance sensor to protect the actual item.

The inspectors should monitor the alarm annunciation in the alarm stations. They should also observe the operation of any interfacing systems, such as CCTV displays and video recorders to determine proper functioning.

The number of areas and sensor types to be tested depends on the available time, importance of the system in the overall protection program, and operating history. The following guidelines are intended to assist the inspector in selecting areas and sensors for testing:

- At least five protected interior areas (rooms/vaults/MAAs) should be tested. Priority should be given to those areas containing the most critical assets.

- At least one of each type of sensor should be tested, if possible, including motion sensors, penetration sensors, and proximity sensors, if used.

- If several tests of the same type of sensor are satisfactory, extensive testing of that sensor in different areas is not necessary. However, if deficiencies are apparent, sufficient testing should be conducted to determine whether there is a systemic weakness.

- Tests should be conducted for selected areas where environmental concerns (noise, electromagnetic interference, temperature and humidity changes) or physical obstructions are likely to degrade sensor performance.

Evaluation

If a detection system is to be effective, the sensors must detect intrusion, the alarm condition must be correctly assessed, and protective forces must be available for a timely response.

Assessing Sensor Performance

The primary objective in evaluating interior intrusion-detection sensors is to determine whether they effectively detect penetration, intrusion, or proximity to protected devices or equipment. Other factors to consider are:

- Do volumetric sensors detect an individual moving at a rate of 1 ft/sec or faster? (see "Assessing Sensor Performance," page A-2).
- Do BMS sensors initiate an alarm when exposed to an external magnetic field or when the switch is moved one inch from the magnet housing?
- Does the sensor layout allow adversaries to circumvent any sensor(s) because of alignment, obstructions, or environmental interference?
- Are there any temporary entry points or penetrations to barriers that could allow undetected intrusion?

Interpreting Results

The following guidelines are provided to assist the inspector in interpreting evaluation results.

- Many interior sensor systems employ redundant or layered protection schemes that rely on a combination of barrier, volumetric, and point protection systems. If any one of these is found to be deficient during testing, this finding should be evaluated in the context of the site-specific protection program objectives and the effectiveness of other complementary systems.
- In some cases, facility tests may indicate sensors are properly calibrated but inspector tests may indicate that the sensors can be defeated or cannot reliably detect intrusion. In such cases, the inspector can reasonably conclude that there are deficiencies in the test and calibration procedures or in the quality assurance program, or both.
- When facility tests and calibrations and the tests conducted by inspectors indicate that sensors are performing according to specifications, the limitations of the test procedures used must still be considered. All modes of defeat and all physical and environmental factors may not have been considered when conducting the tests.
- Sensor performance that does not appear to be in accordance with specifications may simply indicate sensor drift or an alignment problem. However, a systemic deficiency in sensor design, application, or maintenance might also be indicated. If the facility tests indicate sensors are out of calibration, inspectors should consider instructing the facility's technicians to test a representative sample of sensors to determine the extent of the problem.

Special Considerations

Some sensors are sensitive to the size of the intruder. The inspector should request the facility to provide a small person to conduct walk tests. If special equipment is necessary, it should be provided. Often, interior sensors may be located at ceiling height or in relatively inaccessible places (for example, in ductwork or cable chases). Ladders or other aids may be needed.

Related testing or activities, such as those for barriers, card access control systems, CCTVs, or line supervision or tamper indication, are typically conducted concurrently with sensor tests in order to minimize data-collection activities.

Responsibilities

Inspectors: Select areas and sensors for testing. Direct tests and monitor alarm annunciation. Typically, one inspector will be located at the CAS/SAS and one will be with the test team.

Facility: Conduct routine tests. Provide security technicians. Provide test devices and aids, as required. Provide SPOs for security and radios for two-way communication. Provide personnel to conduct testing at the direction of inspectors.

Internal Coordination

Testing should be coordinated to minimize the impact on facility operations and should not result in undue exposure of test personnel to radiological or other health hazards. Testing should also be scheduled to avoid conflicts with other tests involving other topic teams (for example, the protective force topic team).

Security Considerations

All normal security precautions should be taken. Normally, an SPO should be present or observe testing to ensure there is no unauthorized access or activity at the protected location to be tested. In many cases, special security arrangements must be made before opening vaults or alarmed doors. These arrangements should be coordinated in advance to avoid delays during the testing.

Personnel Assignments

Test Director:

Facility Alarm System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- Alarm technician
- Testers
- SPOs to provide security during tests, as necessary

Equipment:

- Radios
- Test devices (for example, infrared target simulator, glass-break detector, audio source)

Safety:

- Follow normal operating procedures
- Complete a safety plan
- Notify the CAS/SAS before testing is conducted
- Station one inspector in the CAS/SAS
- Coordinate to prevent any undesired armed response to alarms by the protective force

Barrier Penetration Sensors

System Description:	BMS sensors, capacitance sensors, vibration sensors, and audio detectors; surface-mounted and coupled to a control device
Intruder Detection Capabilities:	Various, including physical proximity, forced opening, and physical attack using tools
Vulnerabilities:	Bypassing, tampering, substitution

Concerns

BMS Sensors:

- BMS sensors should have the switch mounted to a fixed surface, with the magnet mounted on the movable surface (door or window); capture or substitution of the magnet should be precluded.
- BMS sensors installed in areas posing a potential health hazard (for example, in radiation zones) should have self-checking test circuitry to eliminate the need for personnel to enter the hazardous area to check devices.
- BMS sensors should always be installed on the protected side of the barrier to preclude tampering.
- BMS sensors should be mounted with tamper-resistant hardware to reduce the potential for surreptitious removal.

Capacitance Sensors:

- The capacitance sensor wire or "blanket" should not make contact with any grounded object or surface. Other grounded objects in the vicinity of the protected barrier, or in the presence of liquids on floors or other nearby surfaces, can drastically alter sensor capacitance.
- Control units for capacitance sensors should be located within the protected space to preclude tampering.

Vibration Sensors:

- Vibration sensors should be mounted within or on the protected inner surface of the protected barrier.
- Because there are several types of vibration sensors (piezoelectric, coaxial cable, wire tension, and others), the particular manufacturer's specifications must be consulted to determine sensor detection capabilities and weaknesses.

Audio Detectors:

- Audio detectors must be calibrated carefully to avoid nuisance alarms caused by common background noises (for example, machinery, vehicles, and other alarm signals).
- Audio glass-break detectors should be positioned to face the window(s) they protect.

Types of Tests

- BMS Sensors

  BMS sensors should be tested by opening the protected portal (door, hatch, or window) sufficiently to create an alarm. In general, an opening of one inch or less should generate an alarm. A second test should be conducted by placing a magnet near the BMS. This should also create an alarm since the switch's magnetic field is being disturbed.

- Capacitance Sensors

  Capacitance sensors are tested by approaching the protected surface and making physical contact. An alarm should occur either upon near contact or actual physical contact with the surface.

- Vibration and Audio Detectors

  Because various technologies are employed, the particular manufacturer's performance testing procedures should be followed, and any specified testing devices should be used.

Test Guidelines

- At least two typical zones should be tested.

- Any zones that have potential vulnerabilities because of sensor configuration, location, or environmental or structural concerns should be tested to reveal any exploitable deficiencies.

Checklist

Barrier Penetration Sensors

Interior Sensors

Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Sensitivity test frequency _____

_____

Sensitivity test method _____

_____

Acceptance criteria for sensitivity test _____

_____

False alarm history/records _____

_____

Make/model _____

_____

Tamper switches (transceivers, control units, junction boxes) _____

_____

Tour/Visual Inspection Items

Unprotected/vulnerable entry points present? _____

_____

Sensor location adequate? _____

_____

Sensor coverage adequate? _____

_____

Sensor overlap sufficient? _____

_____

Sensor compatible with structural materials? _____

_____

Sensors compatible (if multiple sensors used)? _____

_____

Obstructions or nuisance alarm sources present? _____

_____

Control unit protected? _____

_____

Data Collection Sheet
Barrier Penetration Sensors – Interior Sensors

Test Method

	Zone Tested	Functional Test	Sensor Type	Alarm Generation Method
1 **2** **3** **4** **5** **6** **7** **8** **9** **10** **11** **12** **13** **14** **15**				
Comments:				

Area Motion Sensors

System Description:	Ultrasonic, microwave, or passive infrared sensor; wall- or ceiling-mounted; coupled to control device; volumetric coverage pattern
Intruder Detection Capabilities:	Walking, slow walking, or running
Vulnerabilities:	Bypassing coverage pattern, target masking, extremely slow movement

Concerns

General:

- Optimum coverage requires direct line of sight. Obstructions such as columns, beams, storage racks, or bins, furniture, or other large objects may prevent detection.
- Sensor transceivers and control units are subject to physical damage and tampering if they are not mounted to be inaccessible or are not covered by another sensor's detection pattern.
- Depending on the type used, sensors are susceptible to false alarms caused by moving objects (for example, fans), electromagnetic radiation, rapid temperature changes, air movement, seismic vibration, and background noise.
- Different sensor types have different coverage patterns (generally fan- or wedge-shaped). Proper overlap and coverage must be considered to ensure that an intruder cannot go over, around, or under the sensor's pattern of coverage.

Ultrasonic Sensors:

- Telephones, public address systems, alarm bells or sirens, and other loud sound sources can create nuisance alarms.
- Moving objects such as machinery, fans, venetian blinds or curtains, and wind-blown paper can create nuisance alarms.
- The sensor is less sensitive to a target moving across the detection zone.

Microwave Sensors:

- Moving objects such as machinery, fans, and venetian blinds or curtains can create nuisance alarms.
- The microwave detection beam can easily penetrate glass, wood, wallboard, and plastic (including water and drainpipes) creating false alarms from moving objects outside the protected space.
- Fluorescent light fixtures in the detection zone can create nuisance alarms.

- The sensor is less sensitive to a target moving across the detection zone, as opposed to moving toward or away from the sensor.
- The sensor is susceptible to masking (insider).

Infrared Sensors:

- Infrared will not penetrate any solid object, including glass. Movement in the area behind any objects in the detection pattern cannot be detected.
- Heat sources such as radiators, electrical motors, and direct sunlight can create nuisance alarms.
- Lights in the vicinity of the transceiver may attract insects thereby creating nuisance alarms.
- The sensor is less sensitive to a target moving toward or away from the sensor.
- The sensor is susceptible to masking (insider).

Video Motion Detection Cameras:

- Detection effectiveness will decrease if minimum light levels are not maintained. Lighting is necessary even when the area is unoccupied.
- The lighting for a video motion detection system must be on an emergency power supply to be effective during a power failure.
- Some video motion cameras allow the CAS operator to define the detection zone. If the defined zone is too small, detection probability may be decreased.
- Video motion detection cameras frequently have difficulty detecting slow-moving objects.
- Video motion detection cameras require direct line-of-sight with no obstruction. If the detection capability is not verified when placed in secure mode, the video motion sensors can be rendered ineffective by blocking the field of view or covering the lens when the system is in access mode.
- Camera can be manipulated to mask intrusions.

Types of Tests

- Sensitivity Walk Test

  Walk tests are used to verify operability and sensitivity of the sensor. This test is performed by slowly walking (1 ft/sec) toward ultrasonic and microwave sensors until an alarm is received. For infrared sensors, the inspector walks slowly across the detection pattern, starting at a point outside the detection zone and proceeding inward until an alarm is received. This test should establish the far end of the sensor coverage pattern (see "Assessing Sensor Performance, page A-2).

- Crossing Walk Test

  This test verifies the ability of the sensor to detect motion along the least sensitive axis of the detection pattern. After the end of the sensor coverage pattern is determined from a sensitivity walk test, a crossing test should be performed by walking across the far end of an ultrasonic or microwave zone and by slowly walking toward the infrared sensor from various points outside the detection zone. Detection should occur before the tester enters the defined protected space or reaches the protected target/object.

- Avoidance Walk Test

  Based on the sensor coverage pattern (oval, wedge, or circle), the inspector should attempt to enter the target zone from a likely entry point (for example, from a doorway, a heating/ventilation/air-conditioning duct, or other weak point in the barrier system) or by walking around the sensor's zone of coverage. This test should verify adequate sensor coverage and overlap to detect movement in the protected space or movement of the target/object.

- Crawl test may be useful, depending on location of detector.

Test Guidelines

- Upon entering the room to be tested, and prior to testing, sufficient time should be allowed to pass for room temperature and airflow to normalize. Observers should be requested to stand away from the area being tested in order to reduce confusion.

- Testing should be conducted on at least two typical zones.

- Any zones that have potential vulnerabilities caused by obstructions or other sources of interference (for example, lighting, moving objects, noise, vibration, or heat sources) should be tested to determine whether exploitable deficiencies exist.

- If there are apparent weaknesses in zone coverage or sensor overlap, these should be tested to determine whether sensor coverage can be circumvented.

- Experience indicates that interior volumetric sensors are most vulnerable to a very slowly moving target entering the detection zone on the least sensitive axis (across the zones for ultrasonic and microwave sensors, and toward or away from infrared sensors).

- Many sensors have alarm indicator lights built into the sensor head. The inspectors may observe these indicators to facilitate testing the coverage patterns or sensor sensitivity. However, the inspectors should also verify that an alarm is received in the CAS/SAS to ensure that the alarm circuit is functional from sensor to annunciation point.

Checklist

Area Motion Sensors

Interior Sensors

Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Sensitivity test frequency _____

_____

Sensitivity test method _____

_____

Acceptance criteria for sensitivity test _____

_____

False alarm history/records _____

_____

Make/model _____

_____

Tamper switches (transceivers, control units, junction boxes) _____

_____

Tour/Visual Inspection Items

Unprotected/vulnerable entry points present? _____

_____

Sensor location adequate? _____

_____

Sensor coverage adequate? _____

_____

Sensor overlap sufficient? _____

_____

Sensor compatible with structural materials? _____

_____

Sensors compatible (if multiple sensors used)? _____

_____

Obstructions or nuisance alarm sources present? _____

_____

Control unit protected? _____

_____

Data Collection Sheet
Area Motion Sensors – Interior Sensors

Test Method

	Zone Tested	Zone Number	Sensitivity Walk	Crossing Walk	Avoidance Walk	Crawl
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
Comments:						

Proximity Sensors

System Description:	Capacitance tuned circuit, point or proximity sensor, blanket or cable and contact configuration
Intruder Detection Capabilities:	Proximity/physical contact
Vulnerabilities:	Tampering with control unit

Concerns

- Some sensors experience "drift" in capacitance sensitivity over time and require regular sensitivity calibration.
- Sensors may be less effective at low temperatures and low sensitivity settings. Sensors are most reliable under temperature-controlled conditions.
- The capacitance sensor wire or "blanket" should not make contact with any grounded object or room surface. Other grounded objects close to the protected items, or liquids on the floor, may drastically alter the capacitance of the sensor.
- Control units for capacitance sensors should be located within the protected room or space to preclude tampering with sensitivity settings.

Types of Tests

- Capacitance sensors are tested by slowly approaching and physically touching the protected object with the hands. In an attempt to simulate an attempted compromise of this system, gloves should be worn to realistically desensitize the system. An alarm should be generated when in proximity to the object or upon physical contact.

Test Guidelines

- The person conducting the tests should remove all metal objects (radios, watch, coins, or a pocketknife) and should not wear steel-toed shoes. Gloves should be worn.
- Testing should be conducted on at least two typical zones.
- Any zones that have potential vulnerabilities (for example, extreme low temperature, surface water, or unprotected metal objects near the protected target) should be tested to reveal any exploitable deficiencies.

Checklist

Proximity Sensors

Interior Sensors

Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Sensitivity test frequency _____

_____

Sensitivity test method _____

_____

Acceptance criteria for sensitivity test _____

_____

False alarm history/records _____

_____

Make/model _____

_____

Tamper switches (transceivers, control units, junction boxes) _____

_____

Tour/Visual Inspection Items

Sensor location adequate? _____

_____

Standing water present? _____

_____

Grounded objects in proximity to protected object? _____

_____

Control unit protected? _____

_____

Complements other sensors? _____

_____

Data Collection Sheet
Proximity Sensors – Interior Sensors

Test Method

	Zone Tested	Zone Number	Approach and Touch
1 **2** **3** **4** **5** **6** **7** **8** **9** **10** **11** **12** **13** **14** **15**			
Comments:			

Part 3

Perimeter CCTV

Part 3

Perimeter CCTV

Objective

The objective is to test the effectiveness of perimeter CCTV systems for providing surveillance and assessment of ground-based intrusions. The most directly applicable requirements are:

Applicability	Order Reference
Category I and II SNM, Vital Equipment, PAs	DOE Manual 5632.1C-1 Chapter VI, Paragraph 5
Classified Matter, LAs	DOE Manual 5632.1C-1 Chapter VI, Paragraph 5
DOE Property and Unclassified Facilities	DOE Manual 5632.1C-1 Chapter VI, Paragraph 5

System Tested

System - Assessment system

Functional Element - Perimeter/exterior CCTV

Components - CCTV cameras, enclosures, towers, transmission lines, interface with intrusion-detection system, and CAS/SAS switching and displays, testing and maintenance of exterior CCTV, lighting

Scenario

During an initial site tour, inspectors should select various CCTV zones for testing, usually in conjunction with the exterior intrusion-detection system test. Zone selection is based on a number of factors, including CCTV layout, fence line and intrusion-detection system layout, perimeter lighting, visual obstructions such as buildings and manmade structures, terrain and vegetation, and system operating history. The objective of the site tour is to identify potential problems created by irregular terrain (ditches, humps, dips), obstructions that block the view of a camera or create strong shadow effects, poor security lighting, poor camera placement or alignment, or improper integration of camera zones with intrusion-detection system zones.

The inspectors should observe the facility's CCTV technicians and SPOs conducting routine operational and calibration tests of CCTV cameras and associated equipment, if possible. Cameras are identified for testing based on the number, type, configuration, and operating history. Test, calibration, and maintenance procedures are observed to determine whether they are consistent with DOE orders and approved SSSPs and if they are an effective means of verifying proper system operation. Although it is desirable to observe

these activities to determine system status and test and maintenance effectiveness, such tests should not be required if they are not part of the normally scheduled system checks.

The inspectors should conduct individual camera testing during both daylight and darkness and, if practicable, at either sunset or sunrise. This is important to verify that the cameras function properly throughout the full range of lighting conditions. Testing generally consists of run tests across the isolation zone between the outer and inner perimeter fence lines to determine whether the automatic camera call-up, following intrusion-detection system activation, is rapid enough to allow observation of an intruder within the camera field of view. In addition, testing is conducted at the far end of the field of view to verify that camera lens selection provides a discernable image at the maximum viewing distance. Other tests are conducted where features of terrain, obstruction, or lighting indicate that CCTV coverage may not be effective. The purpose of these tests is to determine whether an adversary could cross the perimeter isolation zone, or remain in that zone, without being observed.

The inspectors should monitor the camera displays in the CAS and/or SAS, and observe operation of supporting subsystems, such as camera switching, sequencing, video recording, pan-tilt-zoom (PTZ) control, and date/time generation, if used. The inspectors should also observe the interfacing of systems, including automatic call-up of CCTV upon intrusion-detection system activation, CAS/SAS operator actions, and control and direction of response forces based on CCTV assessment of adversary actions.

The number of camera zones selected for testing depends on the time available, the importance of CCTV in the overall assessment system, and the number of potential deficiencies identified during the site tour. The following guidelines are intended to assist the inspector in selecting zones for testing:

- Normally, a minimum of two camera zones should be tested in conjunction with the perimeter intrusion-detection system test. If zone camera configurations vary (for example, cameras facing one another versus cameras that follow in sequence) or if automatic camera call-up differs because of changes in the intrusion-detection system sensors used, a representative sample of each configuration type should be tested.

- If a variety of cameras and camera lenses are employed, a representative sample should be tested.

- If PTZ cameras are used for perimeter surveillance, at least one of these should be checked, particularly if it is the type that automatically shifts to a preset field of view upon intrusion-detection system activation. PTZ cameras should not be the primary means of assessment in a PIDAS.

- If special application cameras are used (for example, very low light level or infrared), at least one should be tested.

- Tests should be conducted for selected zones in which deficiencies are anticipated due to terrain, vegetation, obstructions, or lighting conditions.

- If the initial tests do not indicate problems, and the camera scenes displayed at the CAS/SAS appear to be generally clear and uniform, the inspectors need not test numerous cameras. However, if deficiencies are apparent, the inspectors should collect sufficient data to determine whether the weakness is an isolated problem or a systemic deficiency.

- Tests should be conducted to evaluate speed of camera call-up and assess if any vulnerabilities exist as a result.

Evaluation

The purpose of a CCTV assessment system is to support the intrusion detection and response functions by promptly and accurately assessing alarms (to include verification of nuisance and false alarms), determine adversary actions, and direct protective forces response. The principal factor in evaluating the CCTV system is whether it effectively and reliably provides prompt and complete observation of the perimeter isolation zone, and particularly the area adjacent to the inner perimeter fence line in any zone from which an alarm is received. Other factors to consider in the evaluation are:

- Is the CCTV system the sole or primary means of assessment and observation, or do SPOs observe the perimeter? System requirements (such as automatic camera call-up) vary depending upon the degree of reliance on CCTV.

- Does the camera layout provide complete coverage of the perimeter or are there gaps that could be exploited by an adversary?

- Are there terrain irregularities, visual obstructions, shadows, or lighting deficiencies that create exploitable weaknesses in the camera coverage?

- Does the CAS/SAS display function of the CCTV system adequately support the assessment requirement in terms of speed of camera call-up, resolution, size of monitor display, and video recording, as applicable to system configuration and the availability of other assessment aids?

- Is the CCTV equipment capable of performing properly in all light conditions, day or night?

- Are the monitor displays (if any) in security towers or other guard posts functional and effective for their intended purpose?

- Are environmental concerns adequately addressed for all expected climatic conditions in terms of environmental enclosures, heaters, blowers, wipers, and other such devices?

Interpreting Results

The following guidelines are provided to assist inspectors in interpreting results in the context of overall system performance:

- As with other security elements, a perimeter CCTV system is only as strong as its weakest link. Tests that indicate that an adversary can cross a camera zone without observation, following intrusion-detection system activation, are evidence that the CCTV assessment system is not fully reliable. The significance of this finding must be analyzed in the context of the site-specific protection objectives and the effectiveness of other assessment aids.

- In some cases, facility tests indicate that visual obstructions, lighting deficiencies, or other weaknesses exist in individual camera zones. However, the capability to assess perimeter alarms remains because of partial coverage from an adjacent camera or from direct visual observation. In such cases, the deficiencies are of lesser concern because other assessment aids provide compensation. However, these deficiencies may indicate problems in system design or in the test and maintenance program. Testing and maintenance deficiencies may be attributed to inadequate maintenance procedures, insufficient attention to reported problems, or incomplete procedures for reporting CCTV failure or degradation.

- Facility tests that indicate that cameras are properly calibrated and aligned, in conjunction with tests conducted by inspectors that indicate an intruder can be effectively observed, are evidence that tested portions of the system are operational and maintenance procedures are effective. However, facility tests do not ensure that all modes of defeat have been assessed or that all weather and lighting conditions have been evaluated to maximally stress the system.

- Facility tests that indicate that individual cameras are not operating in accordance with the manufacturer's specifications may simply be an indicator of isolated equipment degradation. However, such deficiencies may be evidence of a system-wide weakness in the maintenance program or a failure of system components due to age. Most camera image tubes have a predictable useful life, after which rapid degradation and failure can be expected. If all of the cameras in the system were installed at the same time, it is likely that camera failures will occur in rapid succession throughout the system. Life cycle planning for the maintenance and replacement of equipment is required to avoid this and should be documented in maintenance procedures.

Special Considerations

Some sites employ specialized camera equipment, such as video motion detection systems or very low-light-level cameras, that have special test requirements. In such cases, inspectors should be sure to familiarize themselves with the manufacturer's instructions for operation, test, and maintenance of the equipment.

Special attention should be paid to nighttime lighting conditions, including shadowed areas and the effects of transient lighting changes due to vehicle headlights and opening of doors. To increase the efficiency of the data-gathering effort, CCTV testing should be integrated with related inspection activities, such as barrier inspections, intrusion-detection system testing, and checks of tamper and line supervision alarms.

Responsibilities

Inspectors: Select cameras for testing. Direct testing and monitor video displays and recording. Typically one inspector will be stationed at the CAS and at least one at the perimeter.

Facility: Conduct routine testing. Provide technicians and test devices, as necessary. Provide radios for two-way communications. Provide security compensatory measures, as required. Provide personnel (normally an SPO) to conduct zone testing at the direction of inspectors.

Internal Coordination

Testing should be scheduled to avoid conflicts with exercises or activities involving other topic teams (primarily the protective force topic team). Daytime testing is typically conducted concurrently with the perimeter intrusion-detection system testing.

Security Considerations

All normal security considerations should be observed. Normally, an SPO must monitor (directly or using CCTV) test activity to ensure that no unauthorized personnel enter the PA.

Personnel Assignments

Test Director:

Facility CCTV System Point of Contact:

Facility Protective Force Representative:

Inspection Team Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- CCTV technicians
- Tester

Equipment:

- Radio
- Contrasting clothing for nighttime tests

Safety:

- Follow normal operating procedures
- Complete a safety plan
- Notify the CAS/SAS before testing is conducted
- Station one inspector in the CAS
- Coordinate prevention of any armed response in the area of test personnel

Perimeter CCTV Testing

System Description: Fixed and PTZ cameras, usually with low-light capability, mounted on pole, tower, or wall; coaxial, fiber optic, cable or microwave transmission; associated switching, display, and recording equipment

Capabilities: Perimeter surveillance and intrusion assessment with ability to discriminate human intruders from animals or other causes of false or nuisance alarms from the perimeter intrusion-detection system

Vulnerabilities: Extreme weather (ice, snow, fog, rain, wind), inadequate security lighting, improper alignment or overlap, and visual obstructions or shadows caused by structures or uneven terrain

Concerns

- Cameras and associated supporting systems (switches, monitors, recorders) are complex devices requiring extensive maintenance and calibration. Certain components (especially camera image tubes) are subject to predictable failure due to age, which may be a system-wide occurrence.

- CCTV capability may be seriously degraded by weather extremes (ice, fog, snow, rain, wind-blown dust). Where extremes are prevalent, environmental housings (blowers, heaters, wipers) should be present and in good working condition.

- If CCTV towers, poles, or wall mounts are not rigid, the cameras are subject to wind-induced vibration, which can cause loss of video assessment capability.

- For outdoor application, cameras should have a broad dynamic range to allow for effective operation during daylight and darkness. Light-limiting and auto-iris capabilities should be provided to compensate for varying background light levels and to minimize "bloom" from bright light sources (perimeter lighting, vehicle headlights).

- Visual obstructions (buildings, vegetation, towers, fences, structures or terrain irregularities) can block camera fields of view, creating the potential for intruders to hide or to cross the isolation zone without being observed. The shadows from such obstructions can also interfere with effective observation.

- Camera image tube and video monitor burn-in can result from constant focus on a high-contrast background (extreme light-to-dark ratio), which degrades camera and video monitor performance.

- If camera placement or alignment is improper, there may be "holes" in the CCTV coverage that permit an unobserved intruder to cross the isolation zone. Additionally, if the field of view of the camera is too long for the camera lens, an intruder at the extreme end of the field of view may not be adequately observed. (Note: Industry requires that the postulated adversary occupy at least five vertical scan lines when standing at the far end of the camera's field of view.)

- If cameras are located outside of PA boundaries (to provide better coverage within intrusion-detection system zones), they may be more vulnerable to tampering.

- Automatic camera call-up on the alarm monitor at the CAS/SAS, upon activation of an intrusion-detection system sensor (if employed), should be sufficiently rapid to observe the intruder before he/she crosses the isolation zone and reaches the inner perimeter fence. Alternatively, the video-recording system (digital or laser disc) should be capable of recording and playing back the camera scene showing the intruder crossing the isolation zone.

- PTZ cameras should have limit switches to preclude their facing directly into bright light sources. Also, if they are called up by intrusion-detection system activation, they should be programmed to automatically position themselves to view the area from which the alarm was received.

Types of Tests

- Functional Test

  A functional test of each camera should be performed from the CAS/SAS by calling up each camera scene to verify that cameras are operating and that a clear image is received. If multiple monitors are used for continuous display (for example, nine-inch sequenced monitors) inspectors should verify their function and sequencing (if employed). Check all PTZ functions for proper operation. Also check video-recording systems.

- Field-of-View Test

  In conjunction with the perimeter intrusion-detection system test, inspectors should conduct field-of-view tests if the far point of the camera field of view appears to be excessively long (that is, a clear image of an intruder cannot be seen at the far end of the camera's field of view). To conduct this test, a person should be positioned at the far end of the field of view and should slowly walk across the isolation zone. This test should also verify that the inner perimeter fence line is within the field of view of each camera that observes the isolation zone.

- Obstruction Test

  A test should be conducted when an identified obstruction or shadow may preclude effective observation. This test is conducted by having a person run to and hide behind the obstruction or in the shadowed area.

- Speed of Response Test

  At a narrow point in the isolation zone, a person should run through the intrusion-detection system sensor zone to the inner perimeter fence line. This test is used to verify that automatic camera call-up and/or video recording is sufficiently rapid to allow observation of the intruder before he can leave the isolation zone and the camera's field of view.

Test Guidelines

- All of the foregoing tests should be conducted during daylight and at night to ensure that lighting is adequate and cameras can function properly in low-light conditions. Additionally, the functional test should be conducted at sunrise or sunset to verify that positioning the camera directly toward the sun doesn't degrade camera functions.

- At a minimum, testing of at least two camera zones should be conducted.

- Obstruction tests should be conducted whenever functional tests indicate that the assessment capability in a camera zone is significantly degraded by the obstruction.

- If a significant number of camera zones (more than 10 percent) exhibit degraded picture quality, maintenance records should be reviewed to determine whether useful camera life limits might have been reached due to not replacing camera image tubes.

Checklist

Exterior Perimeter CCTV System

Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Calibration test frequency _____

_____

Calibration test method _____

_____

Acceptance criteria for calibration test _____

_____

Make/model _____

_____

Environmental protection equipment _____

_____

Special equipment (recorders, PTZ cameras) _____

_____

Maintenance history/records _____

_____

Mounting method (tower, pole, wall)_____

_____

Tamper switches (transmitter, receiver, junction boxes) _____

_____

Tour/Visual Inspection Items

Obstructions present? _____

_____

Shadows present? _____

_____

Terrain level? _____

_____

Zone length OK? _____

_____

PTZ cameras, other cameras? _____

_____

Overlap sufficient? _____

_____

Mounting towers/poles rigid? _____

_____

Lighting adequate? _____

_____

Environmental housings adequate? _____

_____

Data Collection Sheet
Exterior Perimeter CCTV System

Test Method

	Zone Tested	Functional Test	Field of View Test	Obstruction Test	Speed of Response Test
1 **2** **3** **4** **5** **6** **7** **8** **9** **10** **11** **12** **13** **14** **15**					
Comments:					

Part 4

Interior CCTV

Part 4

Interior CCTV Performance Tests

Objective

The objective is to test the effectiveness of interior CCTV systems in providing surveillance and assessment of intruder movement and actions.

(Note: CCTV cameras that are physically located outside but cover the exteriors of portals or emergency exits are included within the scope of this performance test.)

The most directly applicable DOE requirements are:

Applicability	**Order Reference**
Category I and II SNM	DOE Manual 5632.1C-1 Chapter VI, Paragraph 5
Classified Matter	DOE Manual 5632.1C-1 Chapter VI, Paragraph 5
DOE Property and Unclassified Facilities	DOE Manual 5632.1C-1 Chapter VI, Paragraph 5

System Tested

System - Assessment system

Functional Element - Interior CCTV

Components - CCTV cameras, enclosures, mounts, transmission lines, interface with the intrusion-detection system and the CAS/SAS, switching and displays, and testing and maintenance of the interior CCTV

Scenario

The inspectors should select various CCTV zones for testing, usually in conjunction with interior intrusion-detection system tests, during an initial facility tour. Zone selection is based on a number of factors, including CCTV layout, intrusion-detection system configuration, interior lighting, and operating history of the cameras. The inspectors should review building layouts, architectural drawings, and briefly tour the facility to familiarize themselves with the location of protected spaces in relation to camera coverage. This

tour should reveal potential problems created by camera placement, visual obstructions, poor lighting, and improper camera alignment.

The inspectors should observe, whenever possible, the facility's CCTV technicians and SPOs as they conduct routine operational and calibration tests of CCTV cameras and associated equipment. Cameras are selected for testing according to the number, type, configuration, and operating/maintenance history of the units in the system. Test, calibration, and maintenance procedures are observed to determine whether they are consistent with DOE orders and approved SSSP requirements, and whether they are an effective means of verifying proper system operation.

The inspectors should conduct individual camera testing during daylight and darkness and, if practical, verify that cameras function properly throughout the full range of light conditions. Testing generally consists of walk tests within various camera zones to determine whether coverage allows observation of an intruder within the camera's field of view. In addition, testing should be conducted at the most distant end of the field of view to verify that the camera lens provides a discernable image at the maximum viewing distance. Other tests are conducted where camera placement, alignment, obstructions, or lighting conditions indicate that CCTV coverage may not be effective. The purpose of these tests is to determine whether an adversary could enter, exit, or remain within a protected space without being observed.

Inspectors should monitor the camera displays in the CAS and SAS, to observe the operation of supporting subsystems, such as camera switching, sequencing, video recording, PTZ control, and date/time generation. The inspectors should also observe the interfacing of systems, including automatic call-up of CCTV upon intrusion-detection system activation, CAS/SAS operator actions, and control and direction of response forces based on CCTV assessment of adversary actions.

The number of camera zones selected for testing depends on the time available, the importance of CCTV in the overall assessment system, and the number of potential deficiencies identified during the site tour. The following guidelines are intended to assist the inspector in selecting zones for testing:

- A minimum of two camera zones should be tested, normally in conjunction with the interior intrusion-detection system test. If camera configurations vary or if automatic camera call-up differs because of changes in the intrusion-detection system sensors used, a representative sample of each type of configuration should be tested.

- If a variety of camera lenses and focal lengths are employed, a representative sample should be tested.

- If interior PTZ cameras are used, inspectors should check at least one, particularly if it is one that automatically shifts to a preset field of view upon intrusion-detection system activation.

- If special-application cameras are used (for example, very-low-light-level, video motion detection, or infrared), at least one should be tested.

- Inspectors should conduct tests on cameras for which deficiencies are anticipated because of configuration, alignment, obstructions, or light conditions.

- If initial tests do not indicate problems, and the camera scenes displayed at the CAS/SAS appear to be generally clear and uniform, the inspectors need not test numerous cameras. However, if deficiencies are apparent, the inspectors should collect sufficient data to determine whether the weakness is isolated or systemic.

- Procedures should be in place to assure that no obstructions can be placed in the "assessment area" (if none, test to see if boxes or objects can be placed).

Evaluation

The purpose of a CCTV assessment system is to support the intrusion-detection and response functions by promptly and accurately assessing alarms (to include verifying nuisance and false alarms), determine adversary actions, and direct protective force response.

Assessing System Effectiveness

The principal objective in evaluating the CCTV system is to determine whether it effectively and reliably provides prompt and adequate observation of the protected space and the principal entry points. The following points should be considered in the evaluation:

- Is the CCTV system the sole or primary means of assessment and observation, or do SPOs provide visual observation of the area? System requirements (such as automatic camera call-up) vary, depending on the degree of reliance on CCTV.

- Does the camera layout provide complete coverage or are there gaps that could be exploited by an adversary?

- Are there visual obstructions and procedures or lighting deficiencies that create exploitable weaknesses in the camera coverage?

- Does the CAS/SAS display function of the CCTV system adequately support the assessment requirement? Aspects to consider include the speed with which cameras are called up, resolution and size of monitor displays, and video recording.

- Is the CCTV equipment capable of performing properly in all light conditions, day or night?

- Are the monitor displays (if any) at guard posts functional and effective for their intended purpose?

- Are all essential cameras in the system functional (or compensatory measures in place)?

Interpreting Results

The following guidelines are provided to assist inspectors in interpreting results in the context of overall system performance:

- Testing that indicates that an adversary can cross a camera zone unobserved following intrusion-detection system activation is evidence the CCTV assessment system is not fully reliable. The significance of this deficiency must be analyzed in the context of the site-specific protection objectives and the effectiveness of other assessment aids.

- In some cases, facility testing indicates that there are visual obstructions, lighting deficiencies, or other weaknesses in individual camera zones. However, the capability to assess intrusion-detection system

alarms remains because of partial coverage from an adjacent camera or direct visual observation. Although these weaknesses are less serious because of these compensatory measures, they may indicate problems in system design or the test and maintenance program. Test and maintenance deficiencies may be attributed to inadequate maintenance procedures, insufficient attention to reported problems, or incomplete procedures for reporting CCTV failure or degradation.

- Facility testing that indicates cameras are properly calibrated and aligned in conjunction with inspection team testing that indicates an intruder can be effectively observed, is evidence that tested portions of the system are operational and that maintenance procedures are effective. However, such tests do not ensure that all modes of defeat have been assessed or that all conditions have been evaluated.

- Facility testing that indicates individual cameras are not operating in accordance with the manufacturer's specifications may simply be an isolated instance of equipment degradation. However, such deficiencies may also be evidence of a system-wide problem regarding the maintenance program or component aging. Most camera image tubes have a predictable useful life, after which rapid degradation followed by failure can be expected. If all the cameras in the system were installed at the same time, it is likely that camera failures will occur in rapid succession throughout the system. To avoid this multiple failure problem, life cycle planning for the maintenance and replacement of equipment is required, the written details of which should be included in the facility maintenance procedures.

Special Considerations

Some sites employ specialized camera equipment, such as video motion detection systems or very-low-light-level cameras, which have special test requirements. For such equipment, inspectors should familiarize themselves with the manufacturer's instructions.

Special attention should be paid to nighttime and after-hours lighting conditions, including shadowed areas and the effects of transient lighting changes due to vehicle headlights, opening of doors, or other light sources.

Has the system been reviewed for classification? How is the video protected from unauthorized access?

To increase the efficiency of the data-gathering effort, CCTV testing should be integrated with related inspection activities, such as barrier inspections, intrusion-detection system tests, and checks of tamper and line supervision alarms.

Responsibilities

Inspectors: Select cameras for testing. Direct testing and monitor video displays and recording. Typically, one inspector will be stationed at the CAS and at least one with the test team.

Facility: Conduct routine testing. Provide technicians and test devices, as necessary. Provide radios for two-way communications. Provide for security compensatory measures, as required. Provide personnel (normally an SPO) to conduct zone tests at the direction of the inspectors.

Internal Coordination

Testing should be scheduled to avoid conflicts with the activities and performance tests conducted by other topic teams (primarily the protective force topic team). Testing typically should be conducted concurrently with interior intrusion-detection system tests.

Security Considerations

All normal security considerations should be observed. Normally, an SPO must monitor (directly or via CCTV) test activity to ensure that no unauthorized personnel enter protected spaces.

Personnel Assignments

Test Director:

Facility CCTV System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- CCTV technicians
- Tester

Equipment:

- Radio

Safety:

- Follow normal operating procedures
- Complete a safety plan
- Notify the CAS/SAS before conducting any test
- Station one inspector in the CAS
- Arrange to prevent any undesired armed protective force response

Interior CCTV Testing

System Description: Fixed and PTZ cameras, wall or ceiling bracket-mounted; coaxial cable or fiber optic transmission; associated switching, display, and recording equipment

Capabilities: Interior surveillance and intrusion assessment, with ability to differentiate between humans and animals, or other causes of false or nuisance alarms generated by the interior intrusion-detection system

Vulnerabilities: Inadequate lighting, improper alignment or overlap, and visual obstructions

Concerns

- Cameras and associated supporting systems (switches, monitors, and recorders) are complex devices requiring extensive maintenance and calibration. Certain components (especially camera image tubes) are subject to predictable failure as they age. Failure because of aging may be a system-wide occurrence if several cameras were installed at the same time.

- Visual obstructions can block camera fields of view, creating the potential for intruders to hide or to cross the camera zone without being observed.

- Camera image tube and video monitor burn-in can result from constant focus on a high-contrast background (extreme light to dark ratio), which degrades camera and video monitor performance.

- If camera placement or alignment is improper, there may be "holes" in the CCTV coverage that could permit unobserved intruder access. Additionally, if the camera's field of view is too long for the camera lens, an intruder at the extreme end of the field of view may not be adequately observed. (Note: Industry requires the postulated adversary to occupy at least five vertical scan lines when standing at the far end of the camera's field of view.)

- Automatic camera call-up on the alarm monitor at the CAS/SAS upon activation of an intrusion-detection system sensor (if employed) should be rapid enough (no more than two seconds) to observe the intruder before he/she crosses the camera's field of view. Alternatively, the video recording system (digital or laser disk) should be capable of recording and playing back the camera scene showing the intruder crossing the camera zone.

- PTZ cameras should have limit switches so they will not face directly into bright light sources. Also, if PTZ cameras are automatically called up by intrusion-detection system activation, they should be programmed to automatically position themselves to view the area from which the alarm was received.

Types of Tests

- Functional Test

  A functional test of each camera should be performed from the CAS/SAS by calling up each camera scene to verify that all cameras are operating and that a clear image is received. If multiple monitors are used for continuous display, their function and sequencing (if employed) should be verified. Any PTZ functions should also be checked for proper operation, as should video-recording systems.

- Field-of-View Test

  In conjunction with the interior intrusion-detection system test, field-of-view testing should be conducted if the far point of the camera's field of view appears to be excessively long (that is, a discernible image of an intruder cannot be obtained at the far end of the camera field of view). To conduct this test, a person should be positioned at the far end of the field of view and should walk slowly across that field of view. In general, this test should also verify that critical access portals are within the camera's field of view.

- Obstruction Test

  A test should be conducted whenever an obstruction and/or lighting conditions could preclude effective observation. This test is conducted by having a person hide behind the obstruction or in a darkened area.

- Speed of Response Test

  To test for speed of camera response when automatic call-up of a camera upon intrusion-detection system activation is employed, a person should activate an interior sensor and then attempt to rapidly exit the area covered by the camera. This test is used to verify that automatic camera call-up and/or video recording is rapid enough to allow observation before the intruder can leave the camera's field of view.

Test Guidelines

- All the foregoing tests should be conducted under day, night, and overcast conditions to ensure that the cameras can function in all light conditions, as applicable.

- At a minimum, test at least two camera zones, if possible.

- Conduct obstruction tests whenever functional testing indicates that the assessment capability in a camera zone is significantly degraded by an obstruction.

- If a significant number of camera zones (more than ten percent) exhibit degraded picture quality, maintenance records should be reviewed to determine whether useful camera life limits have been exceeded because camera image tubes have not been replaced.

Checklist

Interior CCTV System

Interview Items

Installation location _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

Calibration test frequency _____

_____

Calibration test method _____

_____

Acceptance criteria for calibration test _____

_____

Make/model _____

_____

Camera mounting hardware _____

_____

Special equipment (recorders, low-light-level or PTZ cameras) _____

_____

Maintenance history/records _____

_____

Tamper switches (transmitter, receiver, junction boxes) _____

_____

Tour/Visual Inspection Items

Obstructions present? _____

_____

Zone length OK? _____

_____

PTZ cameras, other cameras? _____

_____

Overlap sufficient? _____

_____

Mounting adequate? _____

_____

Lighting adequate? _____

_____

Data Collection Sheet
Video – Interior CCTV

Test Method

	Zone Tested	Functional Test	Field of View Test	Obstruction Test	Speed of Response Test
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
Comments:					

Part 5

Alarm Processing and Display

Part 5

Alarm Processing and Display

Objective

The objective is to test the effectiveness of alarm processing, annunciation and display at alarm stations. The applicable DOE references are:

Applicability	Order Reference
Category I and II SNM	DOE Manual 5632.1C-1 Chapter VI, Paragraph 5
Classified Matter	DOE Manual 5632.1C-1 Chapter VI, Paragraph 5
DOE Property and Unclassified Facilities	DOE Manual 5632.1C-1 Chapter VI, Paragraph 5

System Tested

System - Alarm station functions

Functional Element - Alarm processing and display equipment

Components - Alarm monitors and displays, alarm printers, recording devices, annunciator panels, related equipment controls, switchers, and equipment testing and maintenance

Scenario

Alarm processing and display equipment encompasses all of the annunciation, monitoring, and display equipment and devices employed at the CAS/SAS. This equipment is used to monitor and record the activity associated with all other active subsystems in the security system including: CCTV, intrusion-detection systems, tamper and line supervision alarms, emergency power supplies, communications equipment, access controls, and search equipment.

Since alarm processing and display functions are directly related to the operation of other subsystems, a specific test of such functions is not conducted. Rather, the inspectors note the effectiveness of displays and annunciations at the CAS/SAS in the course of conducting other tests on intrusion detection, access controls, and other systems. The alarm processing and display functions to be tested depend upon the types of security subsystems in use and the types of annunciation/display equipment used at the CAS and SAS. The inspectors should review building layouts and security system drawings and tour the facility to

familiarize themselves with systems configuration and operations so as to effectively evaluate systems annunciation and display capabilities.

While conducting individual subsystems tests, the inspectors note the effectiveness of annunciation and display of alarms, camera scenes, or status indication for the following subsystems or components:

- interior and exterior intrusion-detection system alarms
- line supervision and tamper-indication alarms
- CCTV display monitors and recording devices
- biometric and/or card access controls
- search equipment (SNM detectors, metal detectors), if appropriate
- power supplies
- activated barriers (smoke, foam)
- remotely operated vehicle barriers and gates.

Any components used to maintain a historical record of alarms, displays, or status indication are also to be reviewed. These include alarm logs maintained by computer memory or on storage media (computer tapes or disks), computer printouts, chart recorders, or video recordings, as appropriate.

Inspectors must also verify that the SAS is properly equipped and operated to serve as a completely functional backup to the CAS. The SAS need not be fully redundant with the CAS (that is, alarm processing and display equipment need not be identical), but it must be capable of performing all required alarm response functions. At some facilities, an alarm condition is annunciated in the SAS only if the CAS operator fails to acknowledge it within a prescribed period. Inspectors may elect to verify the operation of such an alarm annunciation capability.

The following guidelines are intended to assist the inspector in selecting items of equipment for testing:

- Evaluate at least one example of each type of annunciation device, display, status indicator, control device, or recording/logging device, if possible.
- Verify that the system functions under emergency power supply conditions and shows no degradation of alarm processing and display.
- Evaluate CCTV system displays and video-recording capability under conditions of both daylight and darkness.

Evaluation

The purpose of alarm processing and display functions is to ensure the capability of the CAS/SAS to control, monitor, and respond to all components of the facility security systems. These functions directly support the requirements to promptly and accurately assess alarms, provide personnel access controls, determine adversary actions, and direct protective force response.

Assessing System Effectiveness

The principal objective in evaluating the alarm processing and display system is to determine whether it effectively and reliably provides prompt and adequate control and monitoring of critical security systems. Other points to consider in the evaluation are:

- Do all alarms provide clear audible and visual annunciation/display?
- Are there provisions to call the CAS/SAS operator's attention to an alarm-associated camera display?
- Does the monitoring equipment provide for straightforward and easy acknowledgment of all alarms?
- Is the status of all power supplies (normal AC, batteries, and generators) clearly indicated at all times?
- Are video displays and recordings clear and available at the CAS and SAS?
- Are line-supervision and tamper-indication alarms clearly displayed and distinguished from other alarm conditions?
- Are alarm processing and display equipment adequately protected against tampering or physical attack?
- Are scheduled testing and maintenance performed on all alarm processing and display equipment?
- Are invalid or unauthorized keycard (or biometric) access attempts promptly and clearly annunciated?
- Does the system provide a historical log of all keycard or biometric access transactions?
- Are controls for security lighting and emergency power available at the CAS and SAS?
- Are there provisions to ensure that the SAS operator is aware of changes in the status of intrusion-detection systems (for example, from secure to access)?
- Are records of false and nuisance alarms maintained by the system?

Interpreting Results

The following guidelines are provided to assist inspectors in interpreting results in the context of overall system performance:

- The types of alarm processing and display systems in use at DOE contractor facilities vary considerably. This is due to differences in the ages of the systems, the degree of computerization employed, and the size and sophistication of the total site security system. Therefore, considerable judgment must be used in evaluating system effectiveness. The key factors considered are whether displays are prompt, clearly annunciated, and understandable. Human factor concerns are important in determining whether an operator can effectively interact with the system to assess and respond to annunciations and displays.

- Another critical factor in evaluating system adequacy is the ability of the SAS to function as an effective backup to the CAS. In determining this adequacy, the inspector should assess whether the SAS can function in a stand-alone mode to completely and effectively monitor, control, and respond to all critical security system functional elements.

Special Considerations

For those sites that use computer-based alarm processing and display systems, it may be necessary to interview the systems analyst or programmer responsible for system software. Some system anomalies may be due to hardware defects or may be the result of programming errors. Another problem relative to computer-based alarm systems is the control of software and its protection against the insider threat. This problem is such that it requires management support and oversight at the highest level possible.

For CCTV system displays and recorders, testing under conditions of both daylight and darkness is required to evaluate system effectiveness.

In the interest of efficiency in data gathering, system testing should be conducted in conjunction with testing scheduled for CCTV, intrusion-detection systems, access controls, emergency power supplies, and other subsystems of the site security system.

Responsibilities

Inspectors: Select systems for testing. Direct testing and monitor annunciation, displays, and recordings. (Typically, one inspector will be stationed at the CAS and at least one with the test team.)

Facility: Conduct routine tests. Provide technicians and test devices as necessary. Provide radios for two-way communication. Provide security compensatory measures, as required.

Internal Coordination

- Conduct testing concurrently with and as an aspect of other system tests.
- Observe all normal security considerations.

Personnel Assignments

Test Director:

Facility System Point of Contact:

Facility Protective Force Representative:

Safety Coordinator:

Facility Safety Coordinator:

Logistical Requirements

Personnel:

- Protective force representative
- Technicians
- Tester
- Systems analyst or programmer

Equipment:

- Radio

Safety:

- Follow normal operation procedures
- Complete a safety plan
- Notify the CAS/SAS before conducting testing
- Station one inspector in the CAS or SAS
- Test personnel should arrange to prevent any undesired armed protective force response

Alarm Processing and Display Equipment

General Characteristics:	CAS/SAS alarm consoles, alarm annunciators and displays, system status indicators, CCTV monitors and recorders, personnel and vehicle access controls, lighting and emergency power controls, and various support equipment
Capabilities:	Security system monitoring, control, assessment, and historical recording, as appropriate; redundant command and control capabilities at CAS and SAS
Vulnerabilities:	Poor man-machine interface, excessive numbers or differing types of displays, inadequate redundancy between CAS and SAS

Concerns

- High numbers of nuisance/false alarms may degrade operator response to bonafide alarm conditions.

- Failures of the system to adequately identify alarm type and specific location may degrade response. This is usually most evident in systems that do not clearly differentiate between tamper-indication or line-supervision alarms, or when multiple sensors are monitored by a single circuit (for example, alarms in series).

- In older systems, which do not use a computer-based integrated alarm processing system, a variety of different alarm panels and status indicators may be employed. This can cause inefficiency and confusion in assessing and acknowledging alarms because the operator must respond to several stand-alone annunciators.

- In older computer-based systems, problems may arise from the computer's lack of speed or from inadequate alarm prioritization. In those cases, the system is unable to expeditiously and effectively sort significant quantities of simultaneous, or near simultaneous, alarm information and the system becomes bogged down resulting in slower alarm processing, caching of alarms without prioritization, or (in the worst case) a system crash. If such conditions were to occur, the ability of the operator to provide timely detection/assessment information to the protective force would be severely degraded, as would the protective force's ability to rapidly respond.

- For computer-based systems, problems may also arise as new or additional sensors or access control devices are added over time. Each time the system configuration changes, software programming changes are required in the system. Unless software modifications and system configuration are carefully controlled, program errors may be generated.

Types of Tests

- Function Test

  Inspectors should perform a functional test of each type of alarm annunciator, status indicator, or control device in conjunction with each subsystem test (for example, CCTV, intrusion-detection system, access control, emergency power test). The purpose of each test is to verify proper system function and to determine whether alarm annunciation, acknowledgement, and command/control are clear and straightforward. Promptness of alarm display following field device activation should be checked concurrently.

- Historical Record Test

  Evaluate any historical records maintained by the system (for example, alarm logs, access control transaction histories, and video recordings) for completeness and accuracy. False and nuisance alarm rates may also be assessed by reviewing these records.

- SAS Test

  Test a representative number of alarm annunciations and command/control functions at the SAS to determine that the SAS provides adequate backup to the CAS. As part of this testing, inspectors should verify that the SAS is capable of knowing about any command actions taken by the CAS that change alarm points or access control devices from the secure mode to the access mode or that enable/disable security devices.

Test Guidelines

- Conduct testing of alarm processing and display in conjunction with other system tests.
- Test CCTV displays and recording capabilities during both daylight and darkness.
- At a minimum, test at least one of each type of alarm annunciation, recording device, and command/control function.
- Conduct a separate limited scope performance test of the SAS to verify its adequacy as a backup to the CAS.

Checklist

Alarm Processing and Display Equipment

Installation Items

Installation location(s) _____

_____

Operational test frequency _____

_____

Operational test method _____

_____

System acceptance criteria _____

_____

Makes/models (CCTV display/recorders, alarm annunciation, card access control) _____

_____

Maintenance history/records _____

_____

CAS/SAS physical protection measures _____

_____

Tour/Visual Inspection Items

Physical protection adequate? _____

_____

Environmental controls/fire protection adequate? _____

_____

Operator's console and controls layout accessible and functional? _____

_____

All displays clear and readable? _____

_____

SAS equipment sufficient? _____

_____

Records storage adequate? _____

_____

Sound level sufficient? _____

_____

Data Collection Sheet
Alarm Processing and Display Equipment

Test Method

	Location Tested (CAS/SAS, Other)	Device/Equipment Tested	Function Tested	Type of Test (Functional Test, Historical Record Test, SAS Test)
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
Comments:				